Legal Opinion on International and Comparative Human Rights Law Concerning the Matter of the Social Card Law Pending before the Constitutional Court of Serbia

I. Interest of the Author Organizations

This legal opinion is presented to A11 Initiative, respectfully, by

1. **Amnesty International**
2. **Centro de Estudios de Derecho, Justicia y Sociedad (Dejusticia)**
3. **Digital Welfare State & Human Rights Project (DWS Project)** based at the **Center for Human Rights & Global Justice at New York University School of Law**
4. **European Roma Rights Center (ERRC)**
5. **Initiative for Social and Economic Rights (ISER)**
6. **Kenya Human Rights Commission (KHRC)**
7. **Program on Human Rights and the Global Economy (PHRGE) & Center for Public Interest Advocacy and Collaboration (CPIAC) at Northeastern University**

and the **secretariat** of **ESCR-Net - International Network for Economic, Social and Cultural Rights** coordinating its elaboration. ESCR-Net connects over 280 NGOs, social movements and advocates across more than 75 countries to build a global movement to make human rights and social justice a reality for all.

The author organizations are individually and collectively amply experienced in both international and regional standards, and strategic litigation of human rights law, including on matters regarding the rights to social security; equality and non-discrimination; privacy; due process; information and participation in public affairs; and remedy.

The author organizations submit that judicial review of the Serbian Social Card Law for compatibility with international human rights law as both vital to affected persons and communities in Serbia, as well as to evolving precedents on digitalization and human rights around the world that the Serbian Constitutional Court's jurisprudence would influence.

Amnesty International is a global movement of more than 10 million people in over 150 countries and territories dedicated to protecting and promoting the rights enshrined in the Universal Declaration of Human Rights and other international treaties throughout the world. Amnesty International has long been at the forefront of protecting internationally recognized social and economic rights worldwide. For instance, under its global Demand Dignity Campaign (2009-2014),[1] Amnesty International contributed to strengthening the legal enforcement of economic, social and cultural rights and to advancing the right to health through research, campaigning, and litigation. Further, Amnesty International has carried out research, produced reports, written submissions and conducted strategic litigation on a range of economic and social rights issues, including rights to health, adequate housing, education and labor rights in many countries across Europe and beyond. In the last year, Amnesty International has also established a new center of expertise, called the Algorithmic Accountability Lab, which examines, confronts and challenges the use of AI and algorithmic systems

[1] For more information on this campaign, see here: https://www.amnesty.org/en/documents/act35/003/2009/en/#:~:text=To%20protect%20the%20rights%20of,move%20from%20acknowledgement%20to%20action.

in the public sector where they stand to impact or violate human rights and access to basic public services. Accordingly, Amnesty International has extensive and global experience and expertise in human rights that are relevant for the determination of this matter including on states' obligations under international law to respect, protect, and fulfill all rights guaranteed in international treaties and the principle of non-discrimination and equality in the enjoyment of all rights, including the right to social security.

The **Centro de Estudios de Derecho, Justicia y Sociedad (Dejusticia)** is a think-do tank in Colombia that contributes to the strengthening of the rule of law and promotes social justice and human rights from a distinctly Global South perspective. As an action-research center, Dejusticia has promoted positive social change for over 15 years by producing in-depth studies and fact-based policy proposals; carrying out effective advocacy campaigns; litigating in the most impactful forums; and designing and delivering training and capacity-building programs. Among its 15 thematic lines and cross-cutting areas, Dejusticia has a Transparency, Technology and Human Rights (TTHR) area that has significant experience in the field of data protection and the relationship between digital technologies and human rights.

The **European Roma Rights Centre (ERRC)** is a Roma-led organization whose vision is for Romani women and men to overcome antigypsyism and its legacy, to achieve dignity, equality, and full respect for their human rights, and to use their experience to contribute to a more just and sustainable world.

The **Initiative for Social and Economic Rights (ISER)** is a non-governmental organization whose main purpose is to ensure the full recognition, accountability and realization of social and economic rights (SERs) in Uganda and in the African region more broadly. ISER conducts extensive research to strengthen the legal, policy and institutional frameworks for the realization of SER. Additionally, it empowers communities to monitor and demand for the realization of SER and seeks redress violations of SER by promoting access to remedies.

The **Kenya Human Rights Commission (KHRC)** is a non-profit organization that works for and safeguards human rights, democratic values, human dignity and social justice in Kenyan society. KHRC uses a multifaceted approach to achieve this mission, including research, public advocacy, monitoring and evaluating government spheres to ensure compliance with human rights, as well as legal services and public interest litigation. KHRC engages Kenyan society through this multiplicity of strategies to reduce powerlessness among poor, vulnerable and marginalized groups in Kenya.

The **Program on Human Rights and the Global Economy (PHRGE)** at **Northeastern University** is a law school program that focuses on the promotion of economic, social and cultural rights within the Northeastern community through the production of cutting-edge scholarship on human rights and through the implementation of legal human rights norms and sound economic development across the world.

The **Digital Welfare State & Human Rights Project (DWS Project)** based at the **Center for Human Rights & Global Justice at New York University School of Law** is a law school project that investigates the human rights impacts of the digital transformation of the state. The project engages in research, action, education, and community building to help ensure that government use of data and digital technologies helps to fulfill economic, social and cultural rights, and does not

become a means of excluding, surveilling, targeting, or punishment, in violation of human rights law and principles.

II. Summary

Judicial review of the Serbian Social Card Law for ensuring compatibility with international human rights law is vital not only to affected persons and communities in Serbia, but also to the maintenance of Serbia's existing obligations under international human rights law. This case also falls within an international context in which courts and international mechanisms are condemning and limiting similar large-scale public sector digitalization initiatives. Judicial review of this law may therefore also influence evolving precedents on digitalization and universal human rights. The author organizations submitting this legal opinion, which individually and collectively possess ample experience in the analysis and litigation of human rights law, therefore submit that this case concerning the Social Card Law is of particular importance in the context of international human rights.

The author organizations submit that in mandating far-reaching digitalization of a national benefits system, Serbia's Social Card Law implicates international human rights to social security; equality and non-discrimination; privacy; due process; information and participation in public affairs; and remedy. These rights are grounded in international instruments ratified by Serbia, including: the International Covenant on Economic, Social and Cultural Rights (ICESCR);[2] the International Covenant on Civil and Political Rights (ICCPR);[3] the European Convention on Human Rights (ECHR),[4] and connected human rights standards.

The Social Card Law unduly restricts the right to social security. The law aims at a much more granular and detailed profiling of beneficiaries' circumstances to achieve a "fairer distribution of social assistance" (Article 3), suggesting that the main aim will be to remove some beneficiaries from the rolls. Its emphasis seems to be particularly on excluding existing recipients and narrowing the beneficiary pool, rather than increasing inclusion and expanding the reach of social programs. Further, the Social Card Law provides for the introduction of automated decision-making within the welfare system, relying on a single, far-reaching registry to ascertain eligibility and ineligibility. But this also risks restricting the right to social security, as such systems all too often increase the risk that individual beneficiaries will not receive benefits to which they are entitled, due to issues of error and bias, among other concerns.

Furthermore, a key purpose of this Law is to consolidate sensitive data from across far-reaching spheres into a single register. This creates an intrusive digital surveillance system, posing severe risks to rights to privacy and data protection. The Social Card Law, in its overbroad reach and vague wording, undermines data rights, including those related to purpose limitation, data minimization, fairness, lawfulness, transparency, accuracy, storage limitation, integrity, confidentiality, data security, non-reliance on solely automated processes, accountability, and oversight.

These impacts will not fall evenly: such human rights harms are consistently experienced more harshly by marginalized groups. Specifically, the effects of the Social Card Law will disproportionately harm

[2] Ratified 12 March 2001.

[3] Ratified 12 March 2001.

[4] Ratified in 2004.

Roma communities, given their overrepresentation in the welfare system, as well as entrenched antigypsyism in Serbia. Interrelated forms of discrimination serve to compound the disadvantages faced among Roma communities in Serbia; a majority live in poverty. Thus, growing evidence that data-driven systems perpetuate inequalities and have discriminatory effects on already marginalized groups suggest that the Social Card Law is likely to reinforce the structural discrimination faced by Roma communities. Moreover, the Law will subject these communities to digital surveillance and arbitrariness in the social benefits system, even as it continues to invisibilize social deprivation and marginalization despite the mass data gathering. The Social Card Law system therefore likely violates the right to equality and non-discrimination.

Digital technologies are often introduced with the promise of making public service delivery more effective and efficient. The Social Card Law in particular is promoted as a tool that will increase administrative efficiency in the welfare system. But this Law, and the digitalized system it envisages and provides for, poses significant human rights risks, which will be borne unevenly, disproportionately impacting marginalized groups, including the Roma community, persons with disabilities, and people living in poverty, who constitute the vast majority of benefits claimants; these harms will be further exacerbated along intersectional lines of identity, such as Roma persons with disabilities living in poverty and Roma women and children.

Cautionary tales of digitized systems impacting the right to social security in Australia, Colombia, India, Kenya, the Netherlands, Poland, Uganda, and the United Kingdom attest to the fact that the legislative flaws and the large-scale human rights risks detailed in this brief are not mere theoretical concerns. The author organizations have provided details about these experiences, and have summarized the outcomes of various court cases regarding these digital systems, in Part IV of this brief for the Court's consideration.

III. The Social Card Law's Incompatibility with International Human Rights Law and Standards

In mandating the far-reaching digitalization of the national benefits system, Serbia's Social Card Law impermissibly undermines international human rights to social security; equality and non-discrimination; privacy; information and participation in public affairs; due process; and remedy. These rights are grounded in international instruments ratified by Serbia including the International Covenant on Economic, Social and Cultural Rights (ICESCR); the International Covenant on Civil and Political Rights (ICCPR); and the European Convention on Human Rights (ECHR),[5] as well as related human rights standards.

This section will first address how the Social Card Law unduly restricts the right to social security by conditioning access on potential beneficiaries' subjection to an exclusionary and intrusive digital surveillance system, containing elements of arbitrary and unaccountable decision-making, in violation of human rights-grounded data principles (section A). It will then address how the impacts of this restriction will disproportionately harm Roma communities within Serbia, who already face structural

[5] Regarding protection of the right to social security in relation to rights guarantees of the European Convention, *see* Council of Europe, Social Security as a Human Rights: The Protection Afforded by the European Convention on Human Rights (2007), available at https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-23(2007).pdf.

discrimination, therefore violatingthe right to equality and non-discrimination (section B). Finally, it will address how the Social Card Law is incompatible with human rights based data protection principles (section C).

A) Undue Restriction of the Right to Social Security

The Social Card Law's design and effects are exclusionary, serving to cut or limit, rather than sustain or increase, coverage and ease of access to social security benefits in Serbia. The purposes of the law, set out in Article 3, are ostensibly to ensure better targeting of social assistance and increase efficiencies. In this regard, the law is more oriented towards exclusion than inclusion: striving to better 'target' social benefits is driven by a desire to ensure a narrower pool of recipients. Where an explicit aim is to better target social protection, it is highly likely that the law will lead to the removal of recipients from the welfare rolls.[6] As such, this represents an undue restriction on the right to social security, impinging on subsequent human rights obligations concerning accessibility, proportionality, transparency and due process, and remedy.

1) Serbia's Obligations under International Human Rights Law Regarding the Right to Social Security

The right to social security is enshrined in a number of international human rights instruments, which Serbia has ratified.[7] At its core, the right aims to aid in poverty reduction, provide means of social inclusion, and guard against circumstances that may lead to social exclusion.[8] It covers the right to access and maintain benefits to secure protection from a range of adverse situations, including a lack of work-related income, unaffordable access to health care, and insufficient family support.[9]

The Universal Declaration of Human Rights provides that the right to social security necessitates, "national and international cooperation" to realize, "the economic, social and cultural rights

---

[6] Universal social protection allows for inclusion of eligibility criteria based on age, disability or unemployment. Several arguments have been made for why schemes offering universal benefits are a desirable way to guarantee the right to social security, in general. The targeting of benefits based on levels of poverty has been criticized for arbitrariness, excluding people who should be covered, stigmatizing effects, and higher administrative costs. *See e.g.* Shahra Razavi, "The case for universal social protection is more self-evident than ever", Development Pathways, 2 June 2020, available at: developmentpathways.co.uk/blog/the-case-for-universal-social-protection-is-more-self-evident-than-ever; Isabel Ortiz, "The Case for Universal Social Protection", International Monetary Fund, Finance & Development, December 2018, available at: imf.org/en/Publications/fandd/issues/2018/12/casefor-universal-social-protection-ortiz; S Kidd and D Athias, Hit and Miss: An assessment of targeting effectiveness in social protection with additional analysis, Working Paper June 2020, available at: https://www.developmentpathways.co.uk/wp-content/uploads/2019/03/Hit-and-miss-longreport-.pdf; Report of the Special Rapporteur on extreme poverty and human rights, A/HRC/38/33, 8 May 2018, available at: https://documents-ddsny.un.org/doc/UNDOC/GEN/G18/127/23/PDF/G1812723.pdf?OpenElement.

[7] E.g., International Covenant on Economic, Social and Cultural Rights, Art. 9. The right to social security is also enshrined in Convention on the Elimination of All Forms of Racial Discrimination, Art. 5(e)(iv); Convention on the Rights of the Child, Art. 26; Convention on the Rights of Persons with Disabilities, Art. 28; and in several Conventions of the International Labor Organization, in particular Convention No. 102 on Minimum Standards of Social Security.

[8] UN Committee on Economic, Social and Cultural Rights (CESCR), *General Comment No. 19: The right to social security (Art. 9 of the Covenant)*, 4 February 2008, E/C.12/GC/19, ¶ 3.

[9] UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The right to social security (Art. 9 of the Covenant)*, 4 February 2008, E/C.12/GC/19, ¶ 2.

indispensable for [individuals'] dignity and the free development of [their] personality."[10] As explained by the United Nations (UN) Committee on Economic, Social and Cultural Rights (CESCR), States Parties have a positive obligation to take effective measures, within the maximum available resources, to "guarantee all peoples a minimum enjoyment of this right."[11] This includes ensuring access to a social security scheme that enables all persons to "acquire at least essential health care, basic shelter and housing, water and sanitation, foodstuffs, and the most basic forms of education, to ensure the right to access of social security systems or schemes on a non-discriminatory basis, especially for disadvantaged and marginalized individuals and groups."[12] The CESCR has further emphasized "the fundamental importance of social security for human dignity."[13]

According to the CESCR's General Comment 19, the right to social security has five essential elements: (1) availability; (2) social risks and contingencies; (3) adequacy; (4) accessibility; and (5) relationship with other rights. Availability refers to the requirement that a social security system be in place to address relevant social risks and contingencies, and the CESCR has stated that public authorities must take responsibility for the effective administration or supervision of the system.[14] Social risks and contingencies require social security systems to provide coverage for the nine principal branches of social security: health care; sickness; old age; unemployment; employment injury; family and child support; maternity; disability; and survivors and orphans.[15] The element of adequacy requires social security systems to be adequate in amount and in duration, allowing beneficiaries to realize their rights to an adequate standard of living. This framework ensures that persons experiencing low-income and significant barriers to education,[16] among other factors, are covered by social security mechanisms. The right to social security thus specifically addresses people that face marginalization and attempts to remedy that marginalization.[17]

The element of accessibility has five sub-sections: (a) coverage; (b) eligibility; (c) affordability; (d) participation and information; and (e) physical access.[18] Coverage requires social security systems to cover all persons in a non-discriminatory manner.[19] Under eligibility, any qualifying conditions must

---

[10] Universal Declaration of Human Rights, G.A. Res. 217A (III), 3d. Sess. U.N. Doc. A/810, Art. 22. (Dec. 10, 1948),

[11] UN Committee on Economic, Social and Cultural Rights (CESCR), *General Comment No. 19: The right to social security (Art. 9 of the Covenant)*, 4 February 2008, E/C.12/GC/19, ¶4. See also UN Committee on Economic, Social and Cultural Rights, *General Comment No. 3: The nature of states parties' obligations, (Art. 2, ¶1 of the Covenant),* 14 December 1990, E/1991/23, ¶10.

[12] *Id.* at ¶59(a), (b).

[13] *Id.* at ¶41.

[14] *Id.* at ¶ 11.

[15] *Id.* at ¶2.

[16] Education has been found to be a "key factor" influencing participation in the informal economy. *See* Sangheon Lee, Philippe Mercadent and Rafael Diez de Medina, *Women and men in the informal economy: a statistical picture,* International Labor Office, (2018) available at https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms_626831.pdf.

[17] In Serbia, seventy-one percent (71%) of Roma people are employed in the informal economy. Serbia has the highest gap in informality in the West Balkan region. *See* N.M. Blazevski, S. Marnie, and I. Keskine, *The Position of Roma Women and Men in the Labour Markets of the Western Balkans: Micronarratives Report*, United Nations Development Programme, 2018, pp. 7, available at https://www.undp.org/sites/g/files/zskgke326/files/migration/eurasia/RomaEmployment_UNDP_RBEC.pdf.

[18] UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The right to social security (Art. 9 of the Covenant)*, 4 February 2008, E/C.12/GC/19, ¶¶23-27.

[19] *Id.* at ¶23.

be "reasonable, proportionate, and transparent."[20] Additionally, "the withdrawal, reduction or suspension of benefits should be limited and based on grounds that are reasonable, subject to due process, and provided for in the national law."[21] The element of affordability necessitates any costs associated with making contributions to the social security system to be affordable for all, without compromising the realization of other rights.[22] Participation and information refers to the "clear and transparent manner" in which social security recipients should receive information about their benefits.[23] Finally, physical access refers to the right of recipients to receive their benefits in a timely manner. [24]

States must carefully weigh the wide-ranging consequences of any interference with the right to social security, particularly given its interconnection with "the realization of many of the economic, social and cultural rights."[25] State laws and policies relating to social security must be measured for validity against the core components and inclusionary purposes of the right, central to which is the obligation to respect existing social security schemes and protect them from unreasonable interference, as well as the right to due process and to a remedy.[26]

2) The Effect of the Social Card Law on the Right to Social Security in Serbia

The Social Card Law does not live up to these standards on the right to social security, and risks violating Serbia's obligations under international human rights law.

Prior to the introduction of the Social Card Law, CESCR raised concerns to Serbia over the "inadequate coverage and amount of social security benefits" and how this "has led to the ineffectiveness of the social security system in reducing poverty"; furthermore the Committee raised how conditionality attached to social security benefits could "effectively deny access by certain disadvantaged and marginalized groups to social security benefits" and raised concerns over the already complicated administrative procedure required to access support.[27]

Given this context, there are several ways in which the Social Card Law will further impact enjoyment of the right to social security in Serbia. First, the Law allows for both *de jure* and *de facto* restrictions to

---

[20] *Id.* at ¶24.

[21] *Id.*

[22] *Id.*

[23] *Id.* at ¶26.

[24] *Id.* at ¶27.

[25] Muelle Flores v. Perú, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am Ct. H.R. (ser. C), No. 375, ¶187 (Mar. 6, 2019) (citing UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The right to social security (Art. 9 of the Covenant)*, ¶28, 4 February 2008, E/C.12/GC/19).

[26] *See e.g.*, GDPR, ¶59(c), ¶¶19-78, "Before any action is carried out by the State party, or by any other third party, that interferes with the right of an individual to social security the relevant authorities must ensure that such actions are performed in a manner warranted by law, compatible with the Covenant,and include: (a) an opportunity for genuine consultation with those affected; (b) timely and full disclosure of information on the proposed measures; (c) reasonable notice of proposed actions;(d) legal recourse and remedies for those affected; and (e) legal assistance for obtaining legal remedies. Where such action is based on the ability of a person to contribute to a social security scheme, their capacity to pay must be taken into account. Under no circumstances should an individual be deprived of a benefit on discriminatory grounds or of the minimum essential level of benefits as defined in paragraph 59(a)."

[27] United Nations Committee on Economic, Social and Cultural Rights, Concluding Observations on the Third Periodic Report of Serbia, E/C.12/SRB/CO/3, 6 April 2022, para. 50.

existing social protection rights and services, limiting access to the right to social security by restricting coverage and introducing new barriers. The Law does affirm a stated goal of "more efficient exercising of social protection rights and services, fairer distribution of social assistance, improving the efficiency and proactivity of the work of bodies in the field of social protection," (Art 3.), and Article 4 lists "prevention of poverty and elimination of the consequences of social exclusion" as one of the purposes of data processing.

However, as discussed further in the discrimination section below, the Social Card Law does not allow for mechanisms that aim to increase inclusion in the system. Instead, a closer analysis suggests that the data processing and automation contemplated by the Law appear to be designed to exclude existing beneficiaries from the system, rather than making the systems fairer and eradicating poverty. In particular, the law clearly establishes a system to automatically trigger processes that could exclude those who appear to have exceeded the threshold income to be eligible for social benefits. Conversely, it makes no provisions aimed at including new beneficiaries and expanding the reach of social protection, such as responsible collection of community-level data aimed at better identification of structural forms of marginalization and substantiate outreach to provide greater access to benefits. This emphasis on exclusion rather than inclusion will likely impede individuals' right to access social security by further restricting access.

This is a common occurrence in the digitalization of welfare systems, where welfare systems are digitalized as a cost-saving mechanism to increase efficiency of social benefits, but instead are designed to lead to unfair exclusion of beneficiaries.[28] Former United Nations Special Rapporteur (UN SR) on extreme poverty and human rights Philip Alston, following extensive research on "'digital welfare states" in a number of countries, found that:

> "the embrace of the digital welfare state is presented as an altruistic and noble enterprise designed to ensure that citizens benefit from technologies, experience more efficient governance and enjoy higher levels of wellbeing. Often, however, the digitization of welfare systems has been accompanied by deep reductions in the overall welfare budget, a narrowing of the beneficiary pool, the elimination of some services, the introduction of demanding and intrusive forms of conditionality, the pursuit of behavioral modification goals, the imposition of stronger sanctions regimes and a complete reversal of the traditional notion that the State should be accountable to the individual."[29]

Whenever such a restrictive digitalized system such as the Social Card becomes an eligibility requirement to access the social security system, the State must demonstrate that this requirement is "reasonable, proportionate, and transparent."[30] This requires not only that there be a legitimate

---

[28] This is similar to targeting methods such as proxy means tests, which ostensibly improve accuracy, but have been shown to instead promote exclusion. *See e.g.*, Stephen Kidd, Bjorn Gelders, and Dilóa Bailey-Athias, *Exclusion by Design: An Assessment of the effectiveness of the proxy means test poverty targeting mechanism*, Extension of Social Security Working Paper, No. 56, International Labour Association (2017), available at https://www.developmentpathways.co.uk/wp-content/uploads/2017/03/Exclusion-by-design-An-assessment-of-the-effectiveness-of-the-proxy-means-test-poverty-targeting-mechanism-1-1.pdf.

[29] Report of the Special Rapporteur on extreme poverty and human rights, 11 October 2019, A/74/493, ¶5, available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/312/13/PDF/N1931213.pdf?OpenElement.

[30] UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The right to social security (Art. 9 of the Covenant)*, 4 February 2008, E/C.12/GC/19, ¶24.

purpose for the imposition of the eligibility requirement, and that the requirement itself is capable of achieving this purpose, but also that the importance of the stated aim is balanced against the consequences for the rights of affected persons and that less restrictive measures are not available.[31] In instances where the penalty for noncompliance with an eligibility criterion is especially harsh, such as the withdrawal or withholding of social security benefits, then it is for the State Party to demonstrate that such a penalty is reasonable and proportionate.[32]

Therefore, although the Social Card Law states that a key purpose is to enable "more efficient exercising of social protection rights," it may ultimately lead to greater exclusion, in law and in fact, as well as greater uncertainty and discouragement for those seeking assistance through the social protection system. The current UN SR on Extreme Poverty and Human Rights, Olivier de Schutter, has held in clear terms that digitalization initiatives such as those contained in the Social Card Law can have the very opposite effect. He notes that digitalization "may lead to more, not less, uncertainty for vulnerable groups. It can also discourage people from applying because of the reliance of online procedures on algorithms designed to detect fraud, even unrelated to the claiming of the benefit itself."[33] Especially in light of the fact that the Social Card Law may result in the complete denial of benefits from those unable to meet the eligibility requirements, the government has thus far failed to discharge its burden in demonstrating that the use of the Social Card is reasonable, proportionate, or transparent.

Not only might the law lead to *de jure* exclusion, due to the exclusionary design of the law, a second issue is that the Social Card Law's reliance on automated decision-making within the benefits system may lead to *de facto* violations of the right to social security due to technical, administrative, or operational challenges. Article 4 provides for the "Automation of procedures and processes related to acting in the field of social protection" while, as detailed in the data protection section below, Article 17 also envisages automated processes. But the introduction of automated decision-making within welfare systems often increases the risk that individual beneficiaries will not receive benefits to which they are entitled. The significant flaws in data processing described in the data principles section below—in particular the lack of provisions to ensure data accuracy and review mechanisms, the automatization of decisions, and the lack of traceability and explainability of how decisions are made—heighten the risk of wrongful exclusion of beneficiaries through faulty automation. Such errors are frequent in systems that involve the gathering and processing of large amounts of personal data to profile and categorize beneficiaries to make predictions, correlations between certain characteristics, or in general "derive information deemed useful to make decisions."[34] Systems like the Social Card, which seek to bring together large amounts of data across a wide range of categories spanning income, assets, ability to work, and household information, are particularly complex and draw on many

---

[31] UN Committee on Economic, Social and Cultural Rights, *Maribel Viviana López Alban vs. Spain, Views adopted by the Committee under the Optional Protocol to the International Covenant on Economic, Social and Cultural Rights, concerning communication No. 37/2018,* 29 November 2019, E/C.12/66/D/37/2018, ¶11.5.

[32] UN Committee on Economic, Social and Cultural Rights, *Maria Cecilia Trujillo Calero vs. Ecuador, Views adopted by the Committee under the Optional Protocol to the Covenant concerning communication No. 10/2015*, 14 November 2018, E/C.12/63/D/10/2015, ¶12.1.

[33] UN Special Rapporteur on extreme poverty and human rights, 2022 Report on Non-Take Up of Rights in the Context of Social Protection, 19 April 2022, A/HRC/50/38, ¶77.

[34] *Understanding algorithmic decision making: opportunities and challenges*, European Parliament (2019), available at: https://www.europarl.europa.edu/RedData/STUD/2019/624261/EPRS_STU(2019)62461_EN.pdf. *See* also the discussion of the Aadhaar system in Section IV.

different inputs. This complexity increases the chance of error and, crucially, errors in social security systems have serious implications for people's lives.

Further still, automated decision-making in benefits systems such as that envisaged by the Social Card Law seek to rely on a single (far-reaching) registry to ascertain eligibility and ineligibility. As detailed in the data protection section below, the Social Card Law conditions access to benefits to one's subjection to an intrusive system of digital surveillance, and the consolidation of enormous amounts of sensitive data about individuals into a single register. But attempting to represent in a single registry the changing and complicated circumstances of people's lives—particularly the lives of those who are living at the margins and in situations of vulnerability—is an immense challenge.[35] Administrative data is unlikely to always be able to provide accurate and up-to-date information, nor to include those who are the most marginalized, such as undocumented migrants and people without a fixed address. Automation in this context often serves to perpetuate exclusions, and conditioning access in this way may pose an additional barrier to the exercise of the right to social protection.

To provide evidence that these issues have borne out in practice elsewhere, Section IV below describes a number of cases from other jurisdictions where digitalization and automation of large public sector systems led to mass-scale exclusion of beneficiaries and consequent severe implications for human rights, prompting courts to respond. In these ways the Social Card Law severely risks violating the right to social security.

B) **Discriminatory Impacts on Roma Communities**

The Social Card Law risks disproportionately harming Roma communities, given their overepresentation in the social benefits system, entrenched antigypsyism in Serbia, and growing evidence that data-driven systems have discriminatory effects have on already marginalized groups when implemented without sufficient safeguards. The Social Card Law risks reinforcing structural discrimination faced by Roma communities while also subjecting them to digital surveillance and arbitrariness in the social benefits system. Further, despite the consolidation of enormous amounts of information about welfare beneficiaries, the proposed system is likely to continue to invisibilize social deprivation and marginalization.

According to the 2011 census data, there were 147,604 ethnic Roma registered in Serbia, composing 2.1% of the total population on the territory of Serbia (excluding Kosovo and Metohija).[36] However, unofficial sources estimate that the number of Roma in Serbia is significantly higher, in the range of 250,000 to 500,000.[37] According to the research of the Statistical Office of the Republic of Serbia

---

[35] On how excessive targeting can lead to exclusion, see UN Special Rapporteur on extreme poverty and human rights, 2022 Report on Non-Take Up of Rights in the Context of Social Protection, 19 April 2022, A/HRC/50/38, ¶25. ("In particular, excessive targeting increases the complexity of procedures and transforms social workers and administrators into gatekeepers of the system, tasked with avoiding fraud by "undeserving" applicants. Increased complexity entails considerable transaction costs and reduces the take-up by eligible claimants. These exclusionary obstacles run contrary to article 9, as interpreted by the Committee on Economic, Social and Cultural Rights.")

[36] Census of the Population, Households and Dwellings in the Republic of Serbia, (19 November 2012), pp. 2, available at https://publikacije.stat.gov.rs/G2012/PdfE/G201218001.pdf.

[37] Marija Manić, *Serbia: Country Profile 2011-2012,* European Roma Rights Centre, (2013), pp. 7, available at http://www.errc.org/uploads/upload_en/file/serbia-country-profile-2011-2012.pdf.

carried out in 2019 on the situation of women and children, 84% households in the Roma settlements receive some type of cash benefits either financial social assistance, child allowance or one-time financial assistance.[38] Information from the 2019 Serbia Multiple Indicator Cluster Survey (MICS 6) on the situation of women and children shows that five out of six Roma households (83%) live in the conditions of pronounced material deprivation (3 or more factors of material deprivation).[39] The disproportionate representation of the Roma among people needing financial social assistance and therefore living in poverty points to the systemic discrimination against Roma in Serbia.

The European Commission against Racism and Intolerance (ECRI) defines "anti-Gypsyism" as "a specific form of racism, an ideology founded on racial superiority, a form of dehumanisation and institutional racism nurtured by historical discrimination, which is expressed, among others, by violence, hate speech, exploitation, stigmatisation and the most blatant kind of discrimination."[40] The definition of antigypsyism given by ECRI includes the notion of "institutional racism".[41] Institutional racism has been defined most precisely in the United Kingdom, as "the collective failure of an organization to provide an appropriate and professional service to people because of their color, culture, or ethnic origin."[42] Additionally, the Alliance Against Antigypsyism defines the concept as follows:

> Antigypsyism is a historically constructed, persistent complex of customary racism against social groups identified under the stigma 'gypsy' or other related terms, and incorporates: (1) a homogenizing and essentializing perception and description of these groups; (2) the attribution of specific characteristics to them; and (3) discriminating social structures and violent practices that emerge against that background, which have a degrading and ostracizing effect and which reproduce structural disadvantages.[43]

For Roma in Serbia, antigypsyism is not an abstract notion. According to methodologically verified reports and indicators, most Roma are faced with social exclusion and poverty and are exposed to some form of open, and, even more often, covert discrimination.[44]

---

[38] Survey Findings Report: 2019 Serbia Multiple Indicator Cluster Survey (MICS) and 2019 Serbia Roma Settlements Multiple Indicator Cluster Survey, Statistical Office of the Republic of Serbia (October 2020), pp. xxxv, available at https://www.unicef.org/serbia/media/16076/file/MICS%206%20Multiple%20Indicator%20Cluster%20Survey.pdf.

[39] *Id.* at 41.

[40] European Commission against Racism and Intolerance, *General Policy Recommendation No. 13 on Combating Antigypsyism and Discrimination Against Roma,* (2011), pp. 7, available at https://rm.coe.int/ecri-general-policy-recommendation-no-13-on-combating-anti-gypsyism-an/16808b5aee. See also *Vona v Hungary*, European Court of Human Rights, No. 35943/10, Concurring Opinion of Judge Pinto de Albuquerque, (1 July 2013), available at https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-122183%22]}.

[41] European Commission against Racism and Intolerance, *General Policy Recommendation No. 13 on Combating Antigypsyism and Discrimination Against Roma,* (2011), pp. 3, available at https://rm.coe.int/ecri-general-policy-recommendation-no-13-on-combating-anti-gypsyism-an/16808b5aee.

[42] The Stephen Lawrence Inquiry, Report of an inquiry by Sir William MacPherson of Cluny (The MacPherson Report): Chapter 6, pp. 49 (1999) available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/277111/4262.pdf

[43] "Reference Paper on Antigypsyism," Alliance Against Antigypsyism, pp. 1, (16 June 2017), available at https://ergonetwork.eu/wp-content/uploads/2017/12/2017-12-Recommendations-to-fight-antigypsyism.pdf.

[44] "Antigypsyims and cumulative and systemic discrimination constitute the root-causes for [Roma] social exclusion." Goran Bašić, *Roma in the Republic of Serbia: The Challenges of Discrimination,* Minority Righrs Group International, (2021), available at https://minorityrights.org/wp-content/uploads/2021/03/MRG_Rep_RomaSerb_EN_Mar21_E.pdf.

Despite Serbia's efforts to combat antigypsyism,[45] the Roma community in Serbia, "continues to suffer from widespread discrimination, unemployment, forced eviction and de facto housing and educational segregation."[46] CESCR, in its Concluding Observations on the third periodic report of Serbia from April 2022, noted its concern about the "substantive discrimination faced by disadvantaged and marginalized individuals and groups, in accessing work, housing, and education."[47] The Committee urged the State party to "intensify its efforts to promote equality and combat discrimination against Roma and persons belonging to national minority groups, persons with disabilities, refugees, asylum seekers, internally displaced persons, and lesbian, gay, bisexual, transgender and intersex persons."[48]

In particular, CESCR recommended to the State party to:

> "(a) Take the steps necessary to remove all discriminatory legal provisions and adopt the pending anti-discriminatory legislation without delay, and strengthen the enforcement of anti-discrimination legislation, with a view to ensuring the equal enjoyment of economic, social and cultural rights in practice;
> (b) Take measures necessary to ensure that public authorities conduct an equality test when preparing new regulations or policies that have impact on the enjoyment of economic, social and cultural rights by disadvantaged and marginalized individuals and groups, as provided for in the Law on Amendments to the Law on Prohibition of Discrimination;
> (c) Enhance awareness and sensitization, including regarding online hate speech, among public officials and the public."[49]

CESCR also noted failures in Serbia's promotion of the right to social protection.[50] It expressed concern about the, "insufficient budget allocation for social protection as well as the inadequate coverage and the amount of social security benefits overall, which has led to the ineffectiveness of the social security system in reducing poverty."[51] The Committee found that:

> certain conditions attached to social assistance benefits… effectively deny access by certain disadvantaged and marginalized groups to social security benefits. These include the conditioning of parental allowances on certain criteria, such as school attendance and vaccination of children, which has a significant discriminatory effect on Roma families, and the conditioning of financial social assistance on the

[45] The Serbian government officially endorsed the concept of 'antigypsyism and claimed the fight against antigypsyism and racism as one of the key goals of the Strategy for the Roma inclusion in the Republic of Serbia for the period 2022-2030, Official Gazette of the Rep. of Serbia No. 23/2022 (17 Feb. 2022), pp. 61, available at: https://www.minljmpdd.gov.rs/doc/Strategy-for-Social-Inclusion-of-Roma-in-the-Republic-of-Serbia2022-2030-eng.pdf

[46] UN Committee on Civil and Political Rights, *Concluding observations on the third periodic report of Serbia,* 6 April 2022, CCPR/C/SRB/CO/3, ¶ 28.

[47] *Id* at ¶28.

[48] *Id.* at ¶ 29.

[49] *Id.* at ¶¶ 29(a), (b), and (c).

[50] *Id.* at ¶ 50.

[51] *Id.*

> performance of unpaid work. It is also concerned about the complicated administrative procedure for claiming financial social assistance (arts. 9 and 11).[52]

The Committee thus recommended to the State party to:

> (a) Raise the budget allocation for social protection and increase the coverage and amount of social security benefits;
> (b) Review the conditions attached to social assistance benefits, particularly to the parental allowance and financial social assistance, with a view to removing the conditions that are discriminatory or have a discriminatory effect and contradict human rights norms, and take effective measures to improve uptake rates of such benefits;
> (c) Streamline the administrative procedure, with a view to making it easily accessible and user-friendly.[53]

The uncertainty and volatility of eligibility imposed by the Social Card Law may affect the Roma community's access to housing. As noted above, the Social Cards Law's data provisions seem structured to exclude rather than include, as while the law contemplates the collection of over 120 pieces of data related to potential beneficiaries, it invisibilizes indicators that could identify marginalization and social deprivation. In Articles 6 through 10, the Law on Social Cards stipulates which type of applicant's data are collected and processed. However, respective articles do not include data about the applicant's living conditions, although such information could be vital for assessing the socio-economic status of the applicant when deciding on the applicant's right in the field of social protection. Namely, the Government noted in its key policy document on Roma social inclusion that, according to the research carried out in 2019 by the Statistical Office of the Republic of Serbia, around, "32% of substandard Roma settlements (SRS) are not connected to the power grid, while 38% of SRS are not connected to the water supply grid."[54] Similarly, a report resulting from a UN and Serbian government collaborative research initiative found that there are 702 substandard Roma settlements in Serbia with approximately 168.000 inhabitants.[55] Additionally, some 24.000 Roma living in SRS do not have access to electricity, 32.000 Roma do not have access to clean water and about 93.000 Roma have no connection to the sewer network.[56] Unquestionably such living conditions put Roma living in substandard settlements in a particular state of vulnerability and in need of social protection. However,

---

[52] *Id.* at ¶ 51.

[53] *Id.* at ¶¶ 51(a), (b), (c).

[54] Strategy for the Roma inclusion in the Republic of Serbia for the period 2022-2030, Official Gazette of the Rep. of Serbia No. 23/2022 (17 Feb. 2022), pp. 50, available at: https://www.minljmpdd.gov.rs/doc/Strategy-for-Social-Inclusion-of-Roma-in-the-Republic-of-Serbia2022-2030-eng.pdf

[55] UN Office of the High Commisioner of Human Righrs, *Mapping of Substandard Roma Settlements According to Risks and Access to Rights in the Republic of Serbia with Particular Attention to the COVID-19 Epidemic*, Republic of Serbia Social Inclusion and Poverty Reduction Unit, UN Human Rights Team (2020), pp. 3, available at: https://socijalnoukljucivanje.gov.rs/wp-content/uploads/2020/12/Mapiranje_podstandardnih_romskih_naselja_prema_rizicima_i_pristupu_pravima_sa_naroci tim_osvrtom_na_COVID-19.pdf.

[56] UN Office of the High Commisioner of Human Righrs, *Mapping of Substandard Roma Settlements According to Risks and Access to Rights in the Republic of Serbia with Particular Attention to the COVID-19 Epidemic*, Republic of Serbia Social Inclusion and Poverty Reduction Unit, UN Human Rights Team (2020), available at: https://socijalnoukljucivanje.gov.rs/wp-content/uploads/2020/12/Mapiranje_podstandardnih_romskih_naselja_prema_rizicima_i_pristupu_pravima_sa_naroci tim_osvrtom_na_COVID-19.pdf.

according to Articles 6 through 10 of the Law on Social Cards, such information remains invisible in the applicant's social card registry. Thus, despite mandating mass data gathering on potential social welfare beneficiaries, the Social Card Law's data provisions maintains the invisibilization of marginalization that characterizes structural discrimination of Roma communities in Serbia.

This is particularly relevant as Roma are disproportionately affected by evictions, which are characterized by lack of adequate consultations, timely notification of the tenants, lack of any or adequate alternative accommodation, and failure to provide support to stimulate social inclusion.[57] In the most recent case of eviction (2020-2021) of predominantly Romani families from the informal settlement, "Vijadukt," in Rakovica municipality in Belgrade, authorities completely disregarded provisions of the Law on Housing and Building Maintenance concerning displacement of a settlement.[58] In the 2018 evictions of more than 80 Roma living next to the Vinca landfill in Belgrade, some of the families were left without any provision of alternative accommodation.[59]

In addition to this systematic exclusion, Roma people have been unsuccessful within the legal system to redress their injuries. The ERRC provided legal representation before the court to two Romani families who were evicted from their homes in Belgrade in 2012 and placed in an abandoned warehouse in Nis. The Belgrade Court of Appeal rejected the ERRC's argument that forced evictions disproportionately target Roma in Serbia and constitute indirect discrimination. The significant barriers placed on Roma people to access and maintain services such as housing, and to achieve social inclusion more broadly, foreshadow the effects that the Social Card Law could potentially have on this community.

1) The Right to Equality and Non-discrimination

The right to equality[60] is grounded in the principle that all humans, "are born free and equal in dignity and rights."[61] An important component of the right to equality is that States must not only eliminate discrimination but also take positive measures to bring about substantive equality, that is, everyone enjoys economic, social and cultural rights to the same extent.[62] The right to equality and non-discrimination applies to the enjoyment of all rights under the ICESCR and ICCPR, through Article

---

[57] Strategy for the Roma inclusion in the Republic of Serbia for the period 2022-2030, Official Gazette of the Rep. of Serbia No. 23/2022 (17 Feb. 2022), pp. 61, available at: https://www.minljmpdd.gov.rs/doc/Strategy-for-Social-Inclusion-of-Roma-in-the-Republic-of-Serbia2022-2030-eng.pdf

[58] Danilo Ćurčić, *Iskrivljena slika: Ekonomska i socijalna prava u Srbiji,* A11 Initiative (2022), pp. 54-56, available on: https://www.a11initiative.org/wp-content/uploads/2022/05/Izves%CC%8Ctaj%20Iskrivljena%20Slika%20(1)~.pdf?_t=1663934511; *See also* Amnesty International, *Serbia: Roma Still Waiting for Adequate Housing* (2015), available at https://www.amnesty.org/en/wp-content/uploads/2021/05/EUR7013082015ENGLISH.pdf.

[59] "Serbia: Left jobless after eviction from Vinca landfill, Roma begin negotiations with city of Belgrade through EBRD complaint", BUSINESS & HUMAN RIGHTS RESOURCE CENTER, 22 Apr. 2021) https://www.business-humanrights.org/it/latest-news/serbia-left-jobless-after-eviction-from-vinca-landfill-roma-begin-negotiations-with-city-of-belgrade/.

[60] This section draws from Monitoring Working Group, *Collective Position: Data for Economic, Social and Cultural Rights,* International Network for Economic, Social and Cultural Rights (2022), available at: https://www.escr-net.org/sites/default/files/attachments/collective_position_data_2022_complete_en.pdf.

[61] Universal Declaration of Human Rights, G.A. Res. 217A (III), 3d. Sess. U.N. Doc. A/810 (Dec. 10, 1948), Art. 1.

[62] *See*, ESCR-Net Women and ESCR Working Group, *Women and ESCR Working Group briefing paper: the intersection between land and women's economic, social and cultural rights,* International Network for Economic, Social and Cultural Rights, (2016), pp. 1, available at https://www.escr-net.org/sites/default/files/briefing_paper_land_0.pdf.

2 in each, as well as being guaranteed more generally under Article 26 of the ICCPR. Such prohibited discrimination covers grounds on the basis of race, gender, class, and national origin, among other often intersecting classifications.[63] According to the Human Rights Committee, "Article 26 not only entitles all persons to equality before the law as well as equal protection of the law but also prohibits any discrimination under the law and guarantees to all persons equal and effective protection against discrimination" on any protected ground.[64] Article 26, "prohibits discrimination in law or in fact in any field regulated and protected by public authorities."[65] A number of international treaties focus on equality and non-discrimination and these include the Convention on Elimination of Discrimination Against Women, Convention on the Elimination of All Forms of Racial Discrimination, and the Convention on the Rights of the Child.

Article 14 of the ECHR enshrines protections against discrimination in enjoyment of the rights presented in the Convention, the European Court of Human Rights (ECtHR) has established through case law the, "fundamental," nature of the principle of non-discrimination. The ECtHR has found the principle of non-discrimination to be applicable in a number of cases concerning social security including: Andrejeva v. Latvia;[66] Gaygusuz v. Austria;[67] Koua Poirrez v. France;[68] Protocol 12 of the ECHR furthers the protections afforded by Article 14 of the ECHR by allowing for protection against discrimination by a public authority in cases when other convention rights are not engaged and this is in order, "to take further steps to promote the equality of all persons through the collective enforcement of a general prohibition of discrimination."[69] Furthermore, Protocol 12 also introduces a new equality provision that established that, "the principle of non-discrimination does not prevent States Parties from taking measures in order to promote full and effective equality, provided that there is an objective and reasonable justification for those measures."[70]

Part V, Article E of the European Social Charter establishes that, "[t]he enjoyment of the rights set forth in this Charter shall be secured without discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national extraction or social origin, health, association

---

63 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The right to social security (Art. 9 of the Covenant)*, ¶29, 4 February 2008, E/C.12/GC/19, ¶29.

64 UN Committee on Civil and Political Rights, General Comment 18: Non-discrimination, 10 November 1989, HRI/GEN/1/Rev.1, ¶ 1.

65 *Id.* at ¶12.

66 Andrejeva v. Latvia, European Court of Human Rights, ECLI:CE:ECHR (2009) (finding that the deprivation of pension entitlements due to the applicants' lack of Latvian nationality was discriminatory and a violation of the applicants' rights under Article 14 taken in conjunction with Article 1 of Protocol No. 1 and Article 6 of the §1 of the Convention).

67 Gaygusuz v. Austria, European Court of Human Rights, 39/1995/545/631 (1996)(finding that the differential treatment of denial of a pension advance in the form of an emergency assistance to a Turkish national residing in Austria and who had paid unemployment insurance contributions, in violation of Article 14 of the European Convention on Human Rights and Article 1 of Protocol 1 guaranteeing the right to enjoy possessions).

68 Koua Poirrez v. France, European Court of Human Rights, 30/12/2003 (2003) (finding that denial of disability benefits to the applicant due to national origin violated Article 14 of the European Convention on Human Rights taken in conjunction with Article 8).

69 Council of Europe, Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms, Preamble, pp. 2 (2000).

70 *Id.*

with a national minority, birth or other status."[71] This includes the right to social security under Part 2, Article 12.[72]

There are various forms of discrimination. According to the CESCR's General Comment 20, direct discrimination is when a person is treated less favorably than someone else in comparable circumstances.[73] Indirect discrimination is when a practice, rule, policy or requirement is outwardly neutral but has an adverse impact upon a particular group.[74] Formal discrimination exists in states' legal and policy frameworks.[75] Substantive discrimination is experienced in practice, usually by groups who have suffered from historical or persistent prejudice.[76] Discrimination can also be systemic. CESCR notes that "discrimination against some groups is pervasive and persistent and deeply entrenched in social behavior and organization, often involving unchallenged or indirect discrimination."[77] Systemic discrimination is a result of, "legal rules, policies, practices or predominant cultural attitudes in either the public or private sector which create relative disadvantages for some groups, and privileges for other groups."[78]

The right to social security must be enjoyed in law and in practice on the basis of equality and non-discrimination.[79] States should not engage in direct discrimination, guarding against exclusion of structurally marginalized groups, including minorities and Indigenous Peoples, from social security systems, as these are among the, "groups who traditionally face difficulties in exercising their right to

---

[71] Council of Europe, *European Social Charter (Revised)*, 1996, pp. 15, available at https://rm.coe.int/168007cf93.

[72] *Id.* at 7.

[73] UN Committee on Economic, Social and Cultural Rights, *General Comment No. 20: Non-discrimination in economic, social and cultural rights*, 2 July 2009, E/C.12/GC/20, ¶10(a).

[74] *Id.* at ¶10(b). In the European human rights system, for example:

> [I]ndirect discrimination may arise from a neutral rule (Hoogendijk v. the Netherlands (dec.), 2005), from a de facto situation (Zarb Adami v. Malta, 2006, § 76) or from a policy (Tapayeva and Others v. Russia, 2021, § 112).
>
> In D.H. and Others v. the Czech Republic [GC], 2007, the issue was whether the manner in which the legislation was applied in practice resulted in a disproportionate number of Roma children being placed in special schools without justification, and whether such children were thereby placed at a significant disadvantage. The "general policy or measure" that the Court found to be discriminatory was the tests used to evaluate the children's intellectual capacities in order to decide whether to place them in normal or in "special" schools for children with learning disabilities. The test has been designed having in mind the mainstream Czech population and the results were not analysed in the light of the particularities and special characteristics of the Roma children who sat them. This led to indirect discrimination of Roma children who were more likely to perform poorly and were subsequently placed in "special schools" in a disproportionately high number in comparison to children of Czech ethnic origin (§§ 200-201).

Registry of the European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention Prohibition of discrimination, Updated 31 August 2022, ¶¶31-32, available at https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf.

[75] *Id.* at ¶9.

[76] *Id.* at ¶8(a).

[77] *Id.* at ¶12.

[78] *Id.*

[79] UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The right to social security (Art. 9 of the Covenant)*, 4 February 2008, E/C.12/GC/19, ¶29.

social security."[80] For instance, in Trujillo Calero v. Ecuador, the CESCR clarified that States must ensure equality between men and women by ensuring that public policies and legislation accounted for the barriers "experienced in practice by women."[81] The Committee also listed specific instances of said barriers, including, "persistence of stereotypes," which lead women to perform unpaid work at higher frequencies than men.[82]

States must also guard against indirect discrimination in implementing the right to social security. CESCR defines indirect discrimination as "laws, policies or practices which appear neutral at face value, but have a disproportionate impact on the exercise" of economic, social and cultural rights.[83]

2) Discrimination Tied to Digitalization

While automated decision making systems are often touted as neutral, technocratic solutions, a large body of work shows that they have consistently exacerbated inequality.[84] As the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Tendayi Achiume, found, "as 'classification technologies that differentiate, rank, and categorize,' artificial intelligence systems are at their core 'systems of discrimination."'.[85]

Crucially, automated decision-making systems are not deployed evenly across the public sector. Such systems are generally deployed first in those areas where the state interacts with low-income and marginalized groups, such as the criminal justice system, policing, immigration, and welfare systems—and these technologies are often deployed in "uniquely experimental" ways in these spheres[86] and are not, for instance, deployed to detect tax fraud by the wealthy, for example.[87] Similarly, predictive algorithmic systems are deployed within child protective services to try to detect mistreatment of children among low-income families, thereby profiling and monitoring low-income parents, but such

---

[80] UN Committee on Economic, Social and Cultural Rights (CESCR), *General Comment No. 19: The right to social security (Art. 9 of the Covenant)*, 4 February 2008, E/C.12/GC/19, ¶¶¶29, 31, 35.

[81] UN Committee on Economic, Social and Cultural Rights, *Views adopted by the Committee under the Optional Protocol to the Covenant concerning communication No. 10/2015 submitted by Marcia Cecilia Trujillo Calero v. Ecuador*, 14 November 2018, E/C.12/63/D/10/2015, ¶13.3.

[82] *Id.* at ¶13.4.

[83] *Id.* at ¶13.2.

[84] See e.g. Safiya Noble, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM, New York University Press (2018); Virginia Eubanks, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR, St. Martin's Press (2018); Ruha Benjamin, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE, Polity (2019); Rashida Richardson, *Racial Segregation and the Data-Driven Society: How Our Failure to Reckon with Root Causes Perpetuates Separate and Unequal Realities*, 36 BERKELEY TECHNOLOGY LAW JOURNAL, 1051 (2022).

[85] Tendayi Achiume, *Racial Discrimination and Emerging Digital Technologies: a human rights analysis,* Report of the Speical Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance, Human Rights Council,, 18 June 2020, A/HRC/44/57, ¶7.

[86] Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance to the General Assembly, 10 November 2020, A/75/590. See also Report of the Special Rapporteur on extreme poverty and human rights, Visit to the United Kingdom of Great Britain and Northern Ireland, A/HRC/41/39/Add.1, 23 April 2019, at: https://digitallibrary.un.org/record/3806308?ln=en.

[87] Brief by the United Nations Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of the Hague (case number C/09/550982/HAZA 18/388), at https://www.ohchr.org/sites/default/files/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf

automated systems are not used to detect mistreatment within higher-income families.[88] The very deployment of such systems by governments is often itself discriminatory as they tend to disproportionately target and profile marginalized populations.

Further, automated decision-making systems very often result in discrimination due to their design. There are several ways in which algorithmic systems can discriminate.[89] First of all, the gaps and imbalances existing in data that the algorithmic system processes to reach its conclusions often lead to discrimination. Choices around data are not neutral and can lead to different outcomes depending on who has gathered it, what data fields have been included, and how the information is collected. Datasets can therefore be biased and under-representative due to skews and gaps in data collection and this can especially be the case when these datasets are collecting information on marginalized groups. When this data is then processed by algorithmic systems to identify patterns and make predictions, these biases and skews can lead to discriminatory conclusions.

Second, "algorithms reproduce bias embedded in large-scale data sets capable of mimicking and reproducing implicit biases of humans."[90] Datasets generally reflect racial and socioeconomic disparities and realities that are present within society. Thus, the way algorithmic systems are "trained" to draw a certain conclusion may also lead to discrimination, especially when the algorithmic system is trained to detect patterns using data in which the predicted outcome for a particular group is systematically different from other groups and therefore one group is consistently treated differently to others.[91] For example, if a hiring algorithm designed to pick job applicants for interviews is trained on patterns of data of those who previously successfully applied for jobs, it will likely detect and replicate the systemic inequalities in that data. These inequalities may not be related to candidate potential but rather to human and institutional biases that have led to certain marginalized groups being given fewer interviews, and are then replicated by the algorithm.[92]

A further problem arises as algorithmic systems often make decisions based on observing patterns in proxy data. For instance, in 2020 the UK government decided to use an algorithmic system to generate grades for students in England who were unable to sit their A-Level exams due to the COVID-19 Pandemic.[93] A lower grade could lead to a student not being granted a space at their chosen university. The algorithm would use historical data of the grades previous students received from a given school

---

[88] Khiara Bridges, THE POVERTY OF PRIVACY RIGHTS, Stanford University Press (2017); Virginia Eubanks, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR, St. Martin's Press (2018).

[89] *See generally* Giacomo Capuzzo, *A Comparative Study on Algorithmic Discrimination between Europe and North-America*, Italian Ewuality Network, (2022), available at https://www.italianequalitynetwork.it/a-comparative-study-on-algorithmic-discrimination-between-europe-and-north-america/#_ftn62.

[90] Tendayi Achiume, *Racial Discrimination and Emerging Digital Technologies: a human rights analysis,* Report of the Speical Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia, and Related Intolerance, Human Rights Council,, 18 June 2020, A/HRC/44/57, ¶28.

[91] Nina Turner, Paul Resnick, and Genie Barton, *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms,* Brookings Institute (2019), available at https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

[92] *See e.g.,* Jeffrey Dastin, "Amazon scraps secret AI recruiting tool that showed bias against women", REUTERS, (11 October 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.

[93] Will Bedingfield, "Everything that went wrong with the botched A-Levels algorithm", WIRED, (19 August 2020), https://www.wired.co.uk/article/alevel-exam-algorithm.

during their A-Levels. Just under 40% of students received lower grades than was expected.[94] This led to calls that there was a latent algorithmic bias in the system as this made it impossible for some students to be granted top grades despite their teachers predicting they would achieve them. At the same time the rates of top grades at fee-paying schools increased. Following outcry from the public and legal action, the UK Government reversed this decision and allowed students to have grades given to them by their teachers based on their predicted grades and past performance.

Discriminatory outcomes are likely when algorithmic systems use information regarding protected characteristics (e.g. gender, ethnicity, religion).[95] But, even more often, misplaced categories are used as "proxies" for race,[96] ethnicity, gender, and other statuses.[97] For example, an algorithmic system may make decisions based on the "height of a person, which also correlates with gender, or a postcode, which can indirectly indicate ethnic origin in cases of segregated areas in cities, or more directly, a person's country of birth."[98] In these cases, discriminatory decisions can be made about people and whether or not they can access a service based on this proxy indicator which is directly correlated to a factor contributing to structural inequity. In the piloting phase of implementation of the Social Cards Law, between February and August 2022, around 22,000 or more than 10% of the beneficiaries were removed from the social protection system,[99] most of whom were Roma.

Thirdly, digital systems such as the one set up under the Social Cards Law are not well tailored to the needs of the communities who often most rely on these services—as they are not likely to have access to digital systems or be able to interact with them easily. In this sense, digital systems become barriers to their access to social benefits, which according to CESCR, can amount to indirect discrimination; indirect discrimination could be found where States fail to, "remove promptly obstacles which the State party is under a duty to remove in order to permit the immediate fulfillment of a right guaranteed by the Covenant."[100]

C) **Incompatibility with Human Rights-Based Data Protection Principles**

State digitalization efforts must comply with human rights legal standards on privacy; information and public participation; due process; and remedy, which underpin a series of data protection principles. In general, data protection laws address the following aspects: data principles; the rights of individuals in relation to their personal data; legitimate grounds for processing personal data; the obligations of data processors and controllers; accountability and governance structures; and data security considerations. The Social Card Law in Serbia is incompatible with a human rights-based approach to

---

94 Richard Adams, Sally Weale and Caelainn Barr, "A-Level results: almost 40% of teacher assessments in England downgraded", THE GUARDIAN, (13 August 2020), https://www.theguardian.com/education/2020/aug/13/almost-40-of-english-students-have-a-level-results-downgraded.

95 *#BigData: Discrimination in data-supported decision-making*, European Union Agency for Fundamental Rights (2018), pp. 5 available at https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making.

96 Amnesty International, *Xenophobic Machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal,* (2021), p. 20, available at https://www.amnesty.org/en/documents/eur35/4686/2021/en/.

97 See Cathy O'Neill, Weapons of Math Destruction (Broadway Books: 2016), esp. 17-18, 146.

98 *#BigData: Discrimination in data-supported decision-making*, European Union Agency for Fundamental Rights (2018), pp. 5 available at https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making.

99 A11 Initiative, *(Anti)social cards)*, 14 October 2022, available at: https://www.a11initiative.org/en/antisocial-cards/.

100 UN Committee on Economic, Social and Cultural Rights, *General Comment No. 19: The right to social security (Art. 9 of the Covenant)*, 4 February 2008, E/C.12/GC/19, ¶65.

data because of its vague and overbroad provisions, centralization of large amounts of data in a single register, introduction of solely automated decision-making systems, and lack of adequate oversight and safeguards. As such, the digitalization imposed by the Social Card Law fails to live up to data protection principles of:

1. purpose limitation;
2. data minimization;
3. storage limitation;
4. integrity, confidentiality, and data security;
5. imposition of solely automated decision making;
6. fairness, lawfulness, transparency, and accuracy;
7. accountability and oversight.

The Social Card Law undermines the rights of data subjects in a number of ways, such as an overbroad design for data collection and processing and ignoring certain rights (such as those of consent and opt-out) while only vaguely referencing other rights (such as in relation to the right to access information). The section below analyzes the Serbian Social Card Law within the framework of the data protection principles put forth by the Council of Europe (CoE) Convention 108+ and the European Union General Data Protection Regulation ("GDPR"), the two leading documents on data protection that have provided a basis for Serbia's own data protection law - the Law on Protection of Personal Data.[101] The terms and concepts employed in this section should be considered a floor, and not a ceiling, of data protection laws. The Social Card Law ignores or is in clear contravention with some of these basic data protection rights.

1) Underpinnings of Data Protection Principles: Rights to Privacy, Information, Public Participation, Due Process, and Remedy

Data protection principles flow from international human rights law regarding privacy; information and public participation; due process; and remedy.

The right to privacy is found in numerous human rights treaties, including the ICCPR (Art. 17) and ECHR (Art. 8).[102] The Human Rights Committee, which oversees the implementation of the ICCPR, defines the right to privacy as the, "right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on

[101] The CoE Convention is binding on Serbia as it is a member of the Council of Europe. In addition, Serbia's data protection law– LPDP– is harmonized with the GDPR, given that this was an obligation of Serbia as an EU member candidate in the process of EU integration. "Provisions of the LPDP mirror the normative provisions of the GDPR in almost all aspects, including provisions regulating the territorial application of the LPDP, legal basis for data processing, privacy by design, data subject rights, security of processing and personal data breach, data protection impact assessments and officers, and the transfer of personal data. *See* Petar Mijatovic, "The State of Serbia's Personal Data Protection Law after two years," PRIVACY TRACKER (18 August 2021), https://iapp.org/news/a/serbian-law-on-personal-data-protection-law-after-two-years-of-implementation-and-harmonization-with-gdpr/#:~:text=Serbia's%20DPA%20is%20authorized%20to,with%20fines%20of%20850%20euros.

[102] The right to privacy is also well-covered in international treaties protecting the rights of specific groups, including: International Convention on the Rights of the Child, Art 16; International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Art 14; International Convention on the Rights of Persons with Disabilities, Art 22.

his honor and reputation."[103] Here, the reference to "unlawful" means that any interference must be provided for in law, and the mention of "arbitrary" entail that any such interference must be in accordance with the aims and provisions of the ICCPR, as well as, "reasonable in the particular circumstances."[104]

According to the UN High Commissioner on Human Rights, "the right to privacy plays a pivotal role in the balance of power between the State and the individual and is a foundational right for a democratic society. Its importance for the enjoyment and exercise of other human rights online and offline in an increasingly data centric world is growing."[105]

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression defines privacy as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals.[106]

Both the ICCPR[107] and International Convention on the Rights of Persons with Disabilities[108] recognize data protection as a core component of the right to privacy. Data protection is commonly defined as the set of safeguards designed to protect personal information, some of which may be sensitive, and which is collected, processed and stored by "automated" means or intended to be part of a filing system.[109] Sensitive data relates to "characteristics such as race or ethnic identity, sexual orientation, political opinions, physical and mental health, disability, criminal convictions or offenses, and biometric and genetic data."[110] The processing of personal data? implicates everyone's rights broadly, but carries "heightened security risks" for "Indigenous peoples, undocumented migrants, sex workers, or for human rights defenders, the collection and disclosure of sensitive data carries heightened security risks."[111] These risks must be mitigated.[112] Data protection frameworks attempt to mitigate these risks, by "balancing the rights of individuals with the legitimate processing of personal data. They permit the processing of personal or sensitive data but impose stricter conditions and additional safeguards for the processing of that data."[113]

---

[103] International Convention on Civil and Political Rights, Art. 17.

[104] UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation,* 8 April 1988, ¶¶3, 4.

[105] United Nations Office of the High Commissioner for Human Rights, The Right to Privacy in a Digital Age, A/HRC/ 48/31, 13 September 2021, ¶ 6.

[106] United Nations General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, A/HRC/23/40, ¶22.

[107] International Covenant on Civil and Political Rights, Art. 17.

[108] International Convention on the Rights of Persons with Disabilities, Art. 22.

[109] "101: Data Protection", Privacy International (12 Oct. 2017), available at https://privacyinternational.org/explainer/41/101-data-protection.

[110] European Union General Data Protection Regulation, Art. 9. *See also* Monitoring Working Group, *Collective Position: Data for Economic, Social and Cultural Rights,* International Network for Economic, Social and Cultural Rights (2022), pp. 71 (citing generally Privacy International, *The Keys to Data Protection: A Guide for Policy Engagement on Data Protection* (2018); Human Rights Council (2018) The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights, Section B. (A/HRC/39/29)).

[111] *Id.*

[112] *Id.*

[113] *Id.*

In its General Comment on the right to privacy, the UN Human Rights Committee stated:

> The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. Data protection laws have been most elaborated at the regional level.[114]

For States using data processing technologies particularly, effective regulation becomes key, given that "governments too often fail to release reliable information on what kind of surveillance systems they use and for what purposes– and often neglect to present evidence on the efficacy of those systems."[115]

Whilst the right to the protection of personal data is not considered to be an autonomous right in the ECHR, the ECtHR has however recognized the importance of the right of the protection of personal data in relation to the right to privacy as guaranteed by Article 8 (Right to respect for private and family life). This includes in S. and Marper vs. the United Kingdom, where it is established by the court that an individual's ethnic or racial identity is a core part of their private life.[116]

These data protection principles are crucial in the current context of mass-scale extraction and processing of personal data that digitalization of social benefits systems may invite. As Privacy International reflects: "advancement in technology has radically improved analytical techniques for searching, aggregating, and cross-referencing large data sets in order to develop intelligence and insights. With the promise and hope that having more data will allow for accurate insights into human behavior, there is an interest and sustained drive to accumulate vast amounts of data. There is an urgent need to challenge this narrative and ensure that only data that is necessary and relevant for a specific purpose should be processed."[117]

Data protection principles also find roots in the right to participate in the conduct of public affairs, a well-established right found in international human rights treaties.[118] The right should be understood in the broadest possible sense to include not just participating in democratic processes, such as elections and referendums, but also in all political processes that affect economic, social, and cultural rights. The UN Human Rights Committee notes that the right to participation "covers all aspects of public administration, and the formulation and implementation of policy at international, national,

---

[114] UN Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family. Home, and Correspondence, and Protection of Honour and Reputation*, 8 April 1988, ¶10, available at https://www.refworld.org/docid/453883f922.html.

[115] UN Human Rights Council, *The right to privacy in the digital age,* 4 August 2022, A/HRC/51/17, pp. 15, available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement.

[116] S. and Marper vs. the United Kingdom, European Court of Human Rights, Nos. 30562/04 and 30566/04 (2008).

[117] *A Guide for Policy Engagement on Data Protection*, Privacy International (2018), pp. 41, available at https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf.

[118] These include the International Covenant on Civil and Political Rights (Art. 25); the Convention on the Elimination of All Forms of Discrimination Against Women (Articles 7, 8, 14 (2); Convention on the Rights of Persons with Disabilities Articles 3 (c), 4 (3), 29, 33(3); International Convention on the Rights of All Migrant Workers and Members of their Families (Articles 41 and 42); International Convention on the Elimination of All Forms of Racial Discrimination (Article 5 c).

regional and local levels."[119] In the context of social security, CESCR states: "[b]eneficiaries of social security schemes must be able to participate in the administration of the social security system."[120]

Those least likely to enjoy their economic, social, and cultural rights are the most likely to be excluded from data and monitoring processes, especially as these processes can be perceived as somewhat technical in nature, as in the case of digital systems.[121] The former UN Special Rapporteur on extreme poverty and human rights, Magdalena Sepulveda, recommends "inclusive mechanisms" that account for the "asymmetries of power" that create a vicious cycle in which those who are least likely to enjoy their rights are also those least able to participate, which in turn can result in a further denial or deprivation of rights because of the missed opportunity to influence and shape the laws, policies, and other interventions that could have positively impacted on their enjoyment of human rights.[122]

Underpinning the right to participation is the right to access to information, which is protected under Article 19 of the ICCPR. In order for citizens to be able to meaningfully participate in public affairs, it is essential that they have access to clear, comprehensive, and reliable information on how decisions are made. This requires public bodies to set-up processes to keep (and disseminate) relevant, consistent, and timely information on each stage of the decision-making process.

The right to due process is another human rights lynchpin of data protection principles. ICCPR Article 14 provides that "all persons shall be equal before the courts and tribunals," and guarantees due process in adjudication of individual rights, including in relation to administrative and civil law--by competent, independent and impartial State courts and tribunals.[123] Due process must be available to, "all individuals, regardless of nationality or statelessness, or whatever their status, whether asylum seekers, refugees, migrant workers, unaccompanied children or other persons, who may find themselves in the territory or subject to the jurisdiction of the State party."[124] Due process rights require courts and tribunals to guarantee fair, public hearings and to do so expeditiously.[125]

States must notify rights holders of any impingement or non-realization of the right to social security, which must be subject to challenge.[126] In ANCEJUB-SUNAT v. Perú,[127] the Inter-American Court of Human Rights found that the Peruvian State had violated pension-holders' right to be "informed, in

---

[119] Human Rights Committee, *General Comment No. 25: The right to participate in public affairs, voting rights, and the right to equal access to public service,* 7 December 1996, CCPR/C/21/Rev/1/Add.7, ¶5.

[120] UN Committee on Economic, Social, and Cultural Rights, *General Comment No. 19: The right to social security (art. 9)*,4 February 2008, E/C.12/GC/19, ¶26.

[121] Monitoring Working Group, *Collective Position: Data for Economic, Social and Cultural Rights,* International Network for Economic, Social and Cultural Rights (2022), pp. 42.

[122] Human Rights Council, Report of the Special Rapporteur on extreme poverty and human rights, Magdalena Sepúlveda Carmona, 22 May 2014, A/HRC/23/36. ¶22.

[123] International Covenant on Civil and Political Rights, 16 December 1966, Treaty Series vol. 999, Art. 14.

[124] UN Human Rights Committee, *General Comment N. 32: Article 14: Right to equality before courts and tribunals and to a fair trial,* 23 August 2007, CCPR/C/GC/32, ¶9.

[125] *Id.* at ¶3.

[126] ANCEJUB-SUNAT v. Perú, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 394, ¶182 (Nov. 21, 2019).

[127] The victims in this case were a group of public workers who, in the face of institutional reorganization of their place of employment, opted for an early retirement incentive package deal, which included the payment of their pensions as if they had not retired early, but the State of Perú refused to pay the pensions as it promised in the Voluntary Retirement incentive program.

an opportune, clear, transparent and complete manner" of the risk of losing their full pension benefits after enrolling in an early retirement program.[128] In Trujillo Calero v. Ecuador,[129] the CESCR found that the author had a legitimate expectation of coverage under an early retirement pension scheme given the contributions she made to the Ecuadorian Social Security Institute;[130] the Committee found that the failure to provide Trujillo Calero with her pension payments violated the right to social security, *inter alia*, because this non-payment had a "significant impact on the author's life plan and her effective enjoyment of the right through a retirement pension."[131]

When it comes to digital systems, the notions of traceability and explainability are essential to ensure due process. Algorithmic systems and the data that drive them are often not made public by data controllers, creating a "black box" effect that prevents any understanding on how the algorithmic is functioning or making decisions.[132] As the Monitoring Working Group notes, "this inherent opacity and lack of transparency frustrates any efforts to make the system more accountable and ultimately fairer."[133] The EU's Ethical Guidelines for Trustworthy Artificial Intelligence list seven key requirements that AI systems should meet, including: human agency and oversight; transparency; diversity, non-discrimination and fairness; and accountability.[134] The requirement of human agency and oversight entails undertaking impact assessments prior to the development of the system; it also involves data users to be able to make "informed, autonomous decisions" on AI systems, to avoid "unfair manipulation, deception, herding and conditioning."[135] As to human oversight, the guidelines suggest different possible approaches to ensure that an AI system "does not undermine human autonomy or causes other adverse effects."[136]

Finally, data protection principles must encompass the right to a remedy. A measure of the efficacy of any human right can be found in the accessibility and effectiveness of the remedies available to enforce the right in the face of a threat or infringement.

The right to an effective remedy is enshrined in multiple international human rights documents. Article 8 of the Universal Declaration of Human Rights states that "Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights…". Similarly, the ICCPR requires States parties to "ensure that any person whose rights or freedoms [as recognized in the Covenant] are violated, shall have an effective remedy," including through access to "a

---

128 *Id.*

129 Ms. Trujillo Calero, the victim in this case, was denied retirement by the Ecuadorian State even though she met the minimum requirement contributions due to an 8-month pause in voluntary payments that has disaffiliated her from the retirement scheme and hence invalidates all of her subsequent voluntary payments.

130 UN Committee on Economic, Social and Cultural Rights, *Marcia Cecilia Trujillo Calero v. Ecuador*, 14 November 2018, E/C.12/63/D/10/2015, ¶¶16.1-16.4.

131 *Id.* at ¶16.3.

132 Monitoring Working Group, *Collective Position: Data for Economic, Social and Cultural Rights,* International Network for Economic, Social and Cultural Rights (2022), pp. 18 (citing Transparency International, *Algorithmic transparency and accountability* (2021), available at https://knowledgehub.transparency.org/helpdesk/algorithmic-transparency-and-accountability.

133 *Id.*

134 High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, European Commission, (2019), available at: https://futurium.ec.europa.eu/en/european-ai-alliance/blog/ethics-guidelines-trustworthy-artificial-intelligence-piloting-assessment-list.

135 *Id.*

136 *Id.*

competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State". Furthermore, States must "ensure that the competent authorities shall enforce such remedies when granted." Under the ICESCR, CESCR has explained that "Covenant norms must be recognized in appropriate ways within the domestic legal order, appropriate means of redress, or remedies, must be available to any aggrieved individual or group, and appropriate means of ensuring governmental accountability must be put in place"[137] This follows one of the Committee's earliest General Comment, in which it affirmed "the enjoyment of the rights recognized [in the ICESCR], without discrimination, will often be appropriately promoted, in part, through the provision of judicial or other effective remedies."[138]

With regard to the access to remedy for violations to the right to social security, the CESCR has stated:

> Any persons or groups who have experienced violations of their right ... should have access to effective judicial or other appropriate remedies at both national and international levels. All victims of violations of the right to social security should be entitled to adequate reparation, including restitution, compensation, satisfaction or guarantees of non-repetition. National ombudspersons, human rights commissions, and similar national human rights institutions should be permitted to address violations of the right. Legal assistance for obtaining remedies should be provided within maximum available resources.[139]

CESCR has also emphasized that any person or groups who are victims of a violation "should have access to effective judicial or other appropriate remedies at both national and international levels. All victims of such violations should be entitled to adequate reparation, which may take the form of restitution, compensation, satisfaction or guarantees of non-repetition."[140] Furthermore, the ECHR provides that "everyone whose rights and freedoms set forth in the Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."[141]

The Council of Europe has also developed guidance for its member states, including Serbia, to ensure that AI systems are aligned with the right to remedy and human rights more broadly. [142] This guidance puts forward obligations of States with respect to the protection and promotion of human rights and fundamental freedoms in the context of algorithmic system, such as:

---

[137] UN Committee on Economic, Social, and Cultural Rights, *General Comment No.* 9, 3 December 1998, E/C.12/1998/24, ¶2.

[138] UN Committee on Economic, Social, and Cultural Rights, *General Comment No.* 3, 14 December 1990, E/1991/23, ¶5.

[139] United Nations Committee on Economic, Social and Cultural Rights, General Comment 3, The Nature of States Parties' Obligations (Art. 2, ¶. 1, of the Covenant), 1990, ¶¶3, 5.

[140] UN Committee on Economic, Social, and Cultural Rights, *General Comment No.* 14*, Right to the Highest Attainable Standard of Health*, 11 August 2000, ¶59.

[141] European Convention on Human Rights, Art. 13, Right to an Effective Remedy.

[142] Recommendation CM/Rec (2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, 1 April 2020, available at https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154; Declaration on the manipulative capabilities of algorithmic processes, 13 February 2019, Decl. 13/02/2019, available at https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b.

(a) regular assessment of "the human rights impacts of individual systems and their interaction with other technologies";
(b) "regular testing, evaluation, reporting and auditing against state-of-the-art standards related to completeness, relevance, privacy, data protection, other human rights, unjustified discriminatory impacts and security breaches before, during and after production and deployment should form an integral part of testing efforts, particularly where automated systems are tested in live environments and produce real-time effects";
(c) "public, consultative and independent evaluations of the lawfulness and legitimacy of the goal that the system intends to achieve or optimize, and its possible effects in respect of human rights";
(d) "immediate rectification" of "any significant restrictions on human rights that are identified during the testing of such systems"[143]

Furthermore, the CoE Human Rights Commissioner elaborated recommendations for States to, *inter alia*, conduct human rights assessments before the adoption of automated systems, and ensure independent oversight including through "a combination of administrative, judicial or quasi-judicial" mechanisms.[144] Both the CoE and the EU are currently developing legally binding regulation on the use of algorithms.[145]

2) Inadequate Purpose Limitation

According to GDPR, any data-collecting entity must clearly define and explain the purpose of the data collection.[146] The purpose must be "specific and legitimate."[147] Additionally, data collection and processing "should be necessary and proportionate" to the stated purpose.[148]

The data collection goals of the Serbian Social Card Law does not adhere to the above standard. One of the law's stated goals is to:

> "determin[e] the socio-economic status of the individual and related persons in order to establish the facts necessary to decide on the right and service in the field of social protection."[149]

---

[143] Recommendation CM/Rec (2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, 1 April 2020.

[144] Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights, Council of Europe Commissioner for Human Rights (2019), available at https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64.

[145] The EU is currently in the process of developing a legally binding AI Act that aims to provide a comprehensive regulation of private and public uses of AI. The Act will classify uses of AI on the basis of their risk - from no or low risk to high risk. While a large quantity of uses will be deemed low or no risk, it foresees regulation of a limited number of high-risk systems and includes technologies for biometric identification and categorisation of natural persons, systems used in the domains of education (e.g. determining access to educational institutions, assessment of students), employment (e.g. recruitment, evaluation of performance), access to and enjoyment of essential private services and public services and benefits, systems used by law enforcement and migration services (e.g. risk assessment, emotion recognition), and access to justice.

[146] General Data Protection Regulation, Recital 39, Principles of Data Processing.

[147] *A Guide for Policy Engagement on Data Protection*, Privacy International (2018) at 39.

[148] United Nations High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29, (3 August 2018), ¶29.

[149] Serbia Social Card Law, Article 4(1), "Purpose of Data Processing"

This and other stated goals lack the specificity required by the purpose limitation principle. As written, the law relies on generalities regarding governmental purposes and use of data-gathering that would seem to allow for a wide range of potential activities. While the law seems to gather a vast array of data, it does not specify which types of data will be processed to meet each of the stated purposes. Article 4(3) states the purpose of "creation of *social policies* through determining the socio-economic status of the individual and related persons *and the wider community*" (our emphasis). However, the law does not explain what types of social policies these are, nor what reports will need to be generated to inform these policies. Article 4(4) states the purpose of "*prevention of poverty* and *elimination of consequences of social exclusion*"(our emphasis). However, there is no explanation of how the Law could further this goal. To the contrary, other provisions in the Law seem to run counter to this purpose, as discussed above. For example, the lack of engagement of data subjects in verifying accuracy of the data about their own situation, as well as the lack of provisions on the right to review decisions that are automatically triggered by the system, are likely to result in widespread cases of people being denied access to social security payments without effective safeguards against arbitrariness, exacerbating, rather than minimizing, social exclusion.

The purpose statement in Article 4(5) is similarly unspecific: "conducting statistical, socio-economic *and other research*, data analyses and preparation of reports *necessary for the performance of tasks* within the competence of the ministry responsible for social issues and veteran and disability protection" (our emphasis). The catchall phrase, "and other research," does not define the purpose or goal of this research, nor does it clearly define what the "performance of tasks" would be.

The law relies on conclusory language to signal adherence to the principle of purpose limitation. Article 18, "Protection, security and storage of data in the Social Card," states that "the processing performed by data users *is proportional to the purpose*, i.e. users process data that are *appropriate, relevant, and limited to what is necessary* in relation to the purpose of the processing, in accordance with the law governing the protection of personal data" (our emphasis). This asserts, but does not explain or specify mechanisms for guaranteeing, legal protection from unreasonable use of data.

3) Inadequate Minimization

Another relevant principle of data protection is data minimization, that is, states should gather and process only data needed to meet the specific purposes identified.[150] A general test to be applied is to assess whether the same aim could be achieved with less data.[151]

The GDPR explains that the collection and processing of data must be "adequate, relevant,"[152] and "proportionate in relation to the legitimate purpose pursued."[153] This requires public authorities to use

[150] Monitoring Working Group, *Collective Position: Data for Economic, Social and Cultural Rights,* International Network for Economic, Social and Cultural Rights (2022), pp. 74 (citing generally Privacy International, *The Keys to Data Protection: A Guide for Policy Engagement on Data Protection* (2018); Human Rights Council (2018) The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights, Section B. (A/HRC/39/29)).
[151] *Id.*
[152] General Data Protection Regulation, Art. 5(1)(c).
[153] Council of Europe, Protocol Convention, Art. 5(1).

the "least intrusive method is used to achieve a legitimate aim."[154] For instance, collecting "extra data" for future purposes or "simply because no thought has been given to whether it's necessary," violates the principle of minimization.[155]

The Serbia Social Card Law seems to rely on overbroad lists of many types of data that each agency could have, as well as catch-all provisions. Article 15, "Data Exchange" states that the Social Card will connect to "software solutions"' managed by the Ministry. It is important for the law to define what "software solutions" means, given the multiple scenarios to which this could refer. For instance, connecting to software solutions could mean using a separate database, entity, or organization that also has access to the information in order to manage it. If this is the case, the Law does not appear to provide for further confidentiality and privacy guarantees. However, it is this type of guessing that the Law should avoid by clearly stating how the data sought to be collected advances its purposes, how this data is going to be processed and stored, and who exactly will have access to this data.

Article 15 also allows the Ministry to connect to multiple state data registers, from which it can download data into the Social Card, including but not limited to:[156]

- Central Population Register
    - Data on "...refugees from the former Yugoslav Republics: personal name, name of one parent; day, month and year of birth; municipality and republic of birth; place and address from which the person fled; date of registration in the Republic of Serbia; place where the person resides in the Republic of Serbia and address of the apartment and UCIN assigned before acquiring the refugee status; from the address register…"
- Register of the Organization for Compulsory Pension and Disability Insurance
- Registers of the Ministry of Internal Affairs
- Registers of the Employment Office
- Registers of the Tax Administration
- Registers of the Republic Geodetic Authority
    - "Data on holder of the right to real estate from the real estate cadastre (data on holder of right– name and surname and UCIN; data on real estate– name of the municipality, name of the cadastral municipality, real estate address, number of cadastral parcel, value of real estate, type of land, manner of the use of land (culture), class of land, plot area, ordinal number of building, manner of use of building, legal status of building, number of special part of building, area, manner of use of special part of the building, burdens, and restrictions and other data)."

The Social Card Law also does not adequately define data subjects and involves the collection of a wide range of personal and sensitive information of individuals who are not even receiving or applying to receive social benefits. The law requires data collection not only of individual applicants, but also of "related persons." Article 2(6) defines related persons as "persons who have a closer or further

[154] Privacy International, *A Guide for Policy Engagement on Data Protection* (2018), pp. 41, available at: https://privacyinternational.org/report/2255/data-protection-guide-complete.

[155] *Id.*

[156] Below is a sampling of some of the agencies listed in the Law, as opposed to a complete list of the data set out in the Law.

kinship, i.e. property relationship, with the individual that is of influence on the exercise of rights."[157] However, it does not explain what a meaningful "influence" would be on the socioeconomic status of a social protection applicant. For instance, Article 6, "Data processed in the Social Card," includes "ex-extramarital partner" within the definition of "related persons." The law does not specify who exactly would fall under the category of ex-partners, for instance how far back in time the system would go, and, in case of more than one extra marital partners, whether it would gather data on all of them. Simultaneously, Article 9, "Common and individual data of persons related to the individual," requires data of related persons, including Article 9(4) ability to earn a living; Article 9(5) data on income generated; Article 9(6) data on real estate he/she owns, among others data items. This would appear to mean that the Ministry could collect data on (one or more) applicant's ex-partners, on their income, real estate, and other socioeconomic factors, and use that to exclude an applicant from receiving social protection given the ex-partner's "influence" on that applicant, regardless of whether the applicant actually benefits from their ex-partner's socioeconomic status. The legislation does not provide any mitigating measures for these scenarios, which are likely to result due to the overbreadth of data being collected.

Finally, the scope of the requested information seems to extend beyond what is necessary to fulfill the purpose laid out in Article (4)(1). For instance, Article 15(3) requires information on:

> "on returnees based on readmission agreements (name, surname, place and date of birth, UCIN, gender, parent's name)."

It is unclear how much of the specific data fields noted in 15(3) would help the data users determine the socioeconomic status of the individual.

4) Inadequate Storage Limitation

Data should not be kept for "longer than necessary for the purpose for which it was originally obtained."[158] Important public policy considerations guard against the indefinite retention of data, namely that "failure to limit the period for which data is stored increases security risks and raises concerns that it could be used for new purposes merely because it is still available and accessible."[159]

The Serbia Social Card Law does not provide consistent parameters for data retention. For example, Article 7 contains twenty-four (24) items of data to be collected, but it only specifies one (1) of those items to be kept "permanently," while referring to the rest of the items under the Article as "general data" to be kept for ten years:

> "The data referred to in paragraph 1, item (2) of this Article[160] shall be kept *permanently* while other general data on the beneficiary shall be kept for ten years from the termination of the right." (our emphasis)

---

[157] Article 2, "Meaning of Terms."

[158] *A Guide for Policy Engagement on Data Protection*, Privacy International, (2018), at 44.

[159] *Id.*

[160] Article 7(2): "unique citizen's identification number (UCIN), i.e. registration number for foreign citizens (EBS) or unique temporary number for persons whose identity is unknown)."

Additionally, the text of the law only imposes a retention timeframe to specific paragraphs in an Article but remains silent as to the other data items included within the same Article. For instance, Article 8 contains six (6) paragraphs, each containing multiple sub-paragraphs of itemized data, but only paragraph one (1) is subject to a timeframe. The legislation either fails to provide an alternate time-frame for the rest of data items listed or risks being applied as providing for the retention of the data indefinitely.

5) Inadequate Guarantees of Integrity, Confidentiality and Data Security

The principles of integrity and confidentiality require that security measures be in place to protect data, including authentication, restricted user access, and pseudonymization and anonymization of data.[161] Strong data security systems and provisions must also be in place to avoid breaches and subsequent data leaks, which can be used to target data subjects. Centralized systems are often subjected to data leaks, whether accidental or as a result of targeted hacking attempts.

While the Serbia Social Card Law has three articles pertaining to this data protection,[162] given the unprecedented scale of the Social Card database, and the fact that this is the sole registry combining personal and extremely sensitive information--for example, on ethnicity, domestic violence, and economic status--more information is needed to assess the validity of these protections.

6) Imposition of Solely Automated Decision Making

Article 22, paragraph 1 of the GDPR states: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." Exceptions to this right include if the data controller is authorized by a law that "lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests." These safeguards "include as a minimum a way for the data subject to obtain human intervention, express their point of view, and contest the decision."[163]

Art 17 of the Law on Social Cards "The process of forming and submitting notifications" provides for automated decision making which have the immediate legal effect of suspending or reducing social benefits:

> "If during the data processing a discrepancy of data on the beneficiary, i.e. related person is determined, a notification shall be prepared and forwarded to the records in the field of social protection…"

As discussed below, this takes place without adequate safeguards and protection of data subjects rights, in particular, lack of human oversight, no means for beneficiaries to express their point of view or contest the decision, as well as safeguard against poor data accuracy, lack of minimization, purpose limitation, and inadequate guarantees related to storage, integrity, confidentiality and accountability.

---

[161] Privacy International, *A Guide for Policy Engagement on Data Protection* (2018), at 45.

[162] Arts. 18, 19, and 20.

[163] European Commission, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, available at https://ec.europa.eu/newsroom/article29/items/612053/en.

Furthermore, the Article goes on to say that the notification would contain instructions for data users (i.e. social welfare authorities) to carry out further checks or to initiate a procedure "*ex officio*" that would influence the "exercise, change, or termination" of social welfare rights. The wording "procedure *ex officio*" seems to imply no 'human involvement' of social welfare authorities in making a determination to start a procedure. The law also does not specify how data subjects will be informed of a decision to conduct a review before it is made and have a chance contest or provide additional information on the matter, which makes the right to remedy less accessible.

As noted below, the data sets and processes that result in a computer-influenced decision "should be documented to the best possible standard to allow for traceability and an increase in transparency. This enables identification of the reasons why an AI-decision was erroneous which, in turn, could help prevent future mistakes."[164] By failing to provide information on how the system would reach a certain conclusion, the law undermines data subjects' right to a remedy.

7) Non-adherence to Principles of Fairness, Lawfulness, Transparency, and Accuracy

Processing of personal data should be fair and transparent and done in a lawful manner, so that data subjects' information is not used in ways they would not expect. The principles of fairness, lawfulness and transparency provide that data subjects should be aware of the myriad ways in which their personal information is being used by data controllers.[165] To be lawful, data processing must conform to the rule of law.[166] Lawful grounds usually include: consent of the data subject, compliance with a legal obligation (including human rights obligations), performance of a contract with the data subject, public interest, and, in some instances, for scientific, historical, and statistical purposes.[167] To be fair, the data collection must be limited to uses that data subjects would "[reasonably] expect."[168] To be transparent, the database and processes--and any conclusion reached on those basis--must be closely tracked and explainable to data subjects and users or to other stakeholders.

Data protection principles require data controllers to communicate with data subjects in "clear and plain language" the ways in which their personal information is processed.[169] If an agency wants to use the data for a different purpose it must seek the person's consent again and identify a legal basis for processing it. Additionally, "natural persons should be made aware of risks, rules, safeguards, and rights in relation to the processing of personal data and how to exercise their rights in relation to such

---

[164] High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, European Commission, (2019), pp. 17 available at: https://futurium.ec.europa.eu/en/european-ai-alliance/blog/ethics-guidelines-trustworthy-artificial-intelligence-piloting-assessment-list.

[165] *A Guide for Policy Engagement on Data Protection,* Privacy International (2018), available at: https://privacyinternational.org.

[166] *Id.* at 37.

[167] *Id.*

[168] *Id.*

[169] *See, e.g.*, General Data Protection Regulation, Recital 39, Principles of Data Processing.

processing."[170] This ensures that the data processing is "based on the free, specific, informed and unambiguous consent" of the data subjects.[171]

The principles of fairness, lawfulness, transparency, and accuracy also implicate the right to privacy. For instance, individuals have "the right to be provided with and to obtain information about how their data is processed (including how and when it is used); the right to object to the processing of their data, or to rectify it; the right to an effective judicial remedy when their rights are breached; and the right to compensation for any damage caused."[172] In the context of automated systems based on the profiling of individuals, people should be informed about the profiling and how it takes place,[173] which means for example of "inferences about sensitive preferences and characteristics, including when derived from data which is not per se sensitive," and should have a right to access, rectify or delete their own data used for profiling.[174]

Data protection laws also make an explicit link to transparency and the right to information and public participation, discussed in the above section. Articles 13 and 14 of the GDPR require that the processing of personal data be transparent. Additionally, Article 8 of the Protocol to the CoE Protocol Convention mandates public authorities that collect personal data of citizens (referred to as "data controller" in the legislation) inform those whose data is being processed of:

> b. the legal basis and the purposes of the intended processing;
> c. the categories of personal data processed;
> d. the recipients or categories of recipients of the personal data, if any; and
> e. the means of exercising the rights (set out in Article 9)

as well as any necessary additional information in order to ensure fair and transparent processing of the personal data."

Furthermore, the European Commission's Ethical Guidelines for Trustworthy AI explains that the dataset, processes and decisions made by AI systems should be:

---

170 *Id.*

171 United Nations High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29, (3 August 2018), ¶ 29; CoE Protocol Convention, Art 5.2

172 Monitoring Working Group, *Collective Position: Data for Economic, Social and Cultural Rights,* International Network for Economic, Social and Cultural Rights (2022), pp. 72 (citing generally Privacy International, *The Keys to Data Protection: A Guide for Policy Engagement on Data Protection* (2018); Human Rights Council (2018) The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights, Section B. (A/HRC/39/29)).

173 Profiling is understood as "automatic data processing techniques that consist of applying a profile to an individual in order to take decisions concerning him or her for purposes of analysing or predicting his or her personal preferences, behaviours, and attitudes." *See* Council of Europe, *Privacy and data protection: Explanatory Memorandum,* 16 April 2014, available at https://www.coe.int/en/web/freedom-expression/privacy-and-data-protection-explanatory-memo. *See also* Privacy International, *Data is Power: Profiling and Automated Decision-Making in GDPR* (2017), available at https://privacyinternational.org/sites/default/files/2018-04/Data%20Is%20Power-Profiling%20and%20Automated%20Decision-Making%20in%20GDPR.pdf.

174 Monitoring Working Group, *Collective Position: Data for Economic, Social and Cultural Rights,* International Network for Economic, Social and Cultural Rights (2022), pp. 72 (citing generally Privacy International, *The Keys to Data Protection: A Guide for Policy Engagement on Data Protection* (2018); Human Rights Council, The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights, Section B. (2018) (A/HRC/39/29)).

- Traceable: "the data sets and the processes that yield the AI system's decision, including those of data gathering and data labeling as well as the algorithms used, should be documented to the best possible standard to allow for traceability and an increase in transparency. This also applies to the decisions made by the AI system. This enables identification of the reasons why an AI-decision was erroneous which, in turn, could help prevent future mistakes. explainability requires that the decisions made by an AI system can be understood and traced by human beings."
- Explainable: "explainability requires that the decisions made by an AI system can be understood and traced by human beings. Whenever an AI system has a significant impact on people's lives, it should be possible to demand a suitable explanation of the AI system's decision-making process. Such explanation should be timely and adapted to the expertise of the stakeholder concerned."[175]

Serbia has a binding obligation to ensure data protection, as it signed and ratified the first legally binding international treaty specific to data protection, CoE Convention 108.[176] The purpose of the Convention is "to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy".[177] With regards to the rights of data subjects, Article 11 of CoE's Modernized Convention states:

> 1. Every individual shall have a right:
>
> a. not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;
>
> b. to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1;
>
> c. to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her;
>
> d. to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms;
>
> e. to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention;

---

[175] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI,* European Commission, (2019), available at: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1.html#Transparency.

[176] This Convention was developed by the Council of Europe, of which Serbia is a member.

[177] Council of Europe, Convention 108: Convention for the protection of individuals with regard to the processing of personal data, Art. 1, (2018), available at https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.

f. to have a remedy under Article 12 where his or her rights under this Convention have been violated;

g. to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Article 15, in exercising his or her rights under this Convention.

Additionally, Article 7 of the Convention addresses data security, requiring that "appropriate security measures" be taken "for the protection of personal data stored in automated data filed against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration, or dissemination."[178]

The Social Card Law also does not address important questions around transparency, explicability and fairness of the automated decision making process embedded in the Social Card system. As recognized in the above-mentioned Guidelines on Automated Individual Decision-making, "[t]he process of profiling is often invisible to the data subject. It works by creating derived or inferred data about individuals – 'new' personal data that has not been provided directly by the data subjects themselves. Individuals have differing levels of comprehension and may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes. Under Article 12.1 of the GDPR the controller must provide data subjects with concise, transparent, intelligible and easily accessible information about the processing of their personal data."[179] The EU Guidelines on Ethical AI further explain that transparency entails documenting and tracing how the data was processed (traceability) and explain the decision reached (explainability).[180] Indeed, one of the biggest problems with automated processes is that the algorithmic systems underpinning them --particularly those that incorporate machine learning--often become "black boxes," with even those who create them unable to determine how and on what basis decisions are made leading to concerns over transparency and the ability of data subjets to access information on how their data is being processed.[181]

The Social Card Law does not provide information on how data will be processed, for instance what types of algorithmic systems, ranking(s) or indicators, if any, would be used to make determinations and trigger decisions that will have immediate, significant effects on those receiving social security payments. Even when there is a human in the loop, social welfare authorities would still rely on reports and information derived from the system to make determinations about benefits claims and may not be able to understand or explain how the data contained in the report was obtained and a certain conclusion reached. Social welfare authorities should be provided adequate information on how the system works and what are the limitations of such systems in order to make informed, critical decisions on the basis of the data and reports provided on social security applicants.

---

178 Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (adopted 18 May 2018) CETS No. 223, Art. 7.

179 Data Protection Working Party, *Guidelines on Automated Individual decision-making and Profiling for the Purposes of Regulation*, European Commission, (2016), available at: https://ec.europa.eu/newsroom/article29/items/612053/en.

180 High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, European Commission, (2019), pp. 17 available at: https://futurium.ec.euro.

181 Mark van Rijmenam, "Algorithms are Black Boxes, That is Why We Need Explainable AI", MEDIUM (4 SEPT. 2019), https://markvanrijmenam.medium.com/algorithms-are-black-boxes-that-is-why-we-need-explainable-ai72e8f9ea5438.

The Social Card Law does not clearly explain how data subjects' information is used, nor how data subjects can access such information. While Article 11 of the Social Card Law states: the natural person to whom the data refers, has the right through the e-Government Portal, *to have an insight* into the right based on the insight into the data of the Social Card, *as well as other rights*, in accordance with the Law on Protection of Personal Data" (our emphasis), the Law does not articulate how exactly the rights set forth in the Serbian Law on data protection are guaranteed in the context of the Social Card system. Furthermore, the right to insight does not specify what may be accessed by data subjects. In addition, access through an e-Government portal does not consider that many welfare beneficiaries may face challenges due to poverty-based digital exclusion and lack of literacy or digital literacy.

Lastly, the principle of accuracy "reaffirms the rights of data subjects to access their personal data, and to correct incomplete, inaccurate or outdated data which should be provided for in a data protection law."[182] This entails that data subjects can access data that is being gathered about them and are able "...to rectify data that is inaccurate or outdated and to delete or rectify data unlawfully or unnecessarily stored."[183]

The processes for ensuring data accuracy under the Serbian Social Card Law are deeply inadequate. The law does not provide due room for data subjects to review and integrate information about their own situation. There is a lack of guidance on the ability to challenge "discrepancy" findings and possible outcomes. This may detrimentally affect the rights of data subjects in relation to (1) ensuring the data on them is accurate and (2) accessing social protection services, which may be limited based on inaccurate data on their socioeconomic status.

8) Inadequate Guarantees of Accountability and Oversight

The principle of accountability holds data users to their responsibilities of, "complying with standards… and provisions provided for in a data protection law."[184] Furthermore, GDPR sets out accountability obligations and standards including through Article 5(2): "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')"; Article 24(1) sets out provisions for the controller to have to be able to demonstrate that they are processing data in compliance with GDPR and that, "measures shall be reviewed and updated where necessary."[185]

Article 10 of the Social Card Law, titled "Technical Data," ensures that metadata, such as "date, time and access of data, data on identity of the data user, and reason and data to be accessed" is recorded for accountability purposes. However, the language is broad in scope and may be difficult to enforce in practice. Article 14, "Manner and access of use of the Social Card," states, "Data users, *in accordance with their own competencies*, access and use the Social Card by authorizing the access to the Social Card or using data from the Social Card…" (our emphasis) Second, the vastness of information at the disposal of data users may obscure instances of misuse. Third, accountability may be hard to ensure when many potential data users have access to the Social Card data. For instance, Article 11, Beneficiaries of Social Card data, states:

---

182 *A Guide for Policy Engagement on Data Protection*, Privacy International, (2018), at 42.

183 United Nations High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/39/29, (3 August 2018), ¶ 30.

184 Privacy International, *A Guide for Policy Engagement on Data Protection* (2018), at 46.

185 EU General Data Protection Regulation.

> The data processed in the Social Card are used by data users in the *authorities responsible for the implementation of social protection*, namely in the social welfare centers, local self-government units *performing entrusted tasks*, the Ministry, the competent authority of the autonomous province for the implementation of social protection, competent republic authority for the activities of the improvement of social protection *and other state administrative authorities and institutions*, in accordance with the law. (our emphasis)

Another major point of concern relates to the "ex officio" procedures triggered through automation. The Council of Europe Recommendations on the human rights impacts of algorithmic systems[186] instruct states to ensure that: "In the design, development, ongoing deployment and procurement of algorithmic systems for or by them, States should carefully assess what human rights and non-discrimination rules may be affected as a result of the quality of data that are being put into and extracted from an algorithmic system, as these often contain bias and may stand in as a proxy for classifiers such as gender, race, religion, political opinion or social origin (...) Particular attention should be paid to inherent risks, such as the possible identification of individuals using data that were previously processed based on anonymity or pseudonymity, and the generation of new, inferred, potentially sensitive data and forms of categorisation through automated means…."

The law does not specify which types of procedures would be fully automated, nor when and under what circumstances they are triggered. It therefore makes it difficult to identify and mitigate adverse and disproportionate impacts of these decisions on specific groups who may see their benefits lost or reduced because of personal characteristics or patterns of behavior that may make them more "at risk" than others to be denied benefits. As stated, these types of systems can reinforce structural inequalities existing within societies, while also being ineffective to actually address fraud and instead imposing overly punitive measures on vulnerable communities.[187] The significance and reach of the decisions that would be automated, both in terms of number of people as well as in terms of the implications on welfare beneficiaries' lives, would certainly warrant an impact assessment. As mentioned above, as it is not clear what training - if any - staff in social welfare authorities will receive in relation to the specificities of automated decision making in social security systems it could be foreseen that it would be difficult for them to meaningfully feed into any potential review or impact assessment of the system. Such assessment should be conducted by seeking inputs and feedback from those who are affected by the decisions. However, the law does not mention any provision or mechanism to assess impacts, let alone providing any space for those who are going to be impacted by it to raise concerns and share feedback that could improve fairness. Even for cases where there is a human in the loop (i.e. where social welfare officers would act on the basis of a notification triggered by the system), it is unlikely that data subjects would be able to guarantee effective oversight given the lack of adequate provisions allowing traceability and explicability. This could be contradictory to provisions that are likely to be included in the upcoming EU AI Act which once in effect will be the most prominent AI regulatory framework in Europe.

---

[186] Recommendation CM/Rec (2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, 1 April 2020, available at https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.

[187] UN Special Rapporteur on extreme poverty and human rights, 2022 Report on Non-Take Up of Rights in the Context of Social Protection, 19 April 2022, A/HRC/50/38, ¶77.

And regardless of whether decisions are automated or involve a human in the loop, the law does not specify a review mechanism for the challenging of decisions.

IV. Insights on Human Rights Impacts of Digitalization From Other Jurisdictions

The author organizations submit that empirical evidence of the impacts of digitized and automated social benefits, welfare, and identification systems in other countries demonstrate how the human rights risks entailed by the Social Card Law in Serbia are more than theoretical concerns. The increase of digitalization and related social exclusion in the jurisdictions noted below illustrate ways in which digitalized systems, such as the one contemplated by the Social Card Law, can lead to human rights violations.

1) Australia's Automated Decision-Making in Benefits Processes

As the following case study on Australia shows, automated decision-making processes in public benefits administration officially known as the Robodebt Scheme, of the kind contemplated in the Serbian Social Card Law, have in some cases violated the human rights of beneficiaries and former beneficiaries by denying access to otherwise eligible beneficiaries due to technical design faults, and by raising barriers to transparency and access to an adequate remedy.

In 2016, the Australian Department of Human Services (DHS) initiated an automated debt recovery system, to identify individuals who were overpaid social security benefits and recover their overpayments.[188] In a departure from prior procedures, where humans investigated possible overpayments, robodebt automated benefits eligibility determinations and radically increased debt letter issuance. In particular, because the system averaged income in its calculations, it falsely accused many individuals with irregular income streams of owing debts. "A social service organization eventually reported that a quarter of the debt notices it investigated were wrong[.]"[189] The government moreover placed the burden of proof on individuals who received debt collection letters to show that they did not owe a debt, in spite of, as the federal court later described, the "profound asymmetry in resources, capacity and information".[190]

"An Australian senate inquiry concluded that 'a fundamental lack of procedural fairness' ran through the entire process."[191] In 2019, Gorden Legal filed a class action lawsuit challenging DHS's use

[188] Joanna Redden, Jessica Brand, and Vanessa Terzieva, "Data Harm Record (Updated)", Data Justice Lab, (August 2020),https://datajusticelab.org/data-harm-record/; *See also* Victoria Legal Aid, "Robo-debts", available at https://web.archive.org/web/20210209080156/https://www.legalaid.vic.gov.au/find-legal-answers/centrelink/robo-debts.

[189] Joanna Redden, "The Harm that Data Do: Paying Attention to How Algorithmic Systems Impact Marginalized People Worldwide is Key to a Just and Equitable Future", SCIENTIFIC AMERICAN, (1 NOV. 2018), https://www.scientificamerican.com/article/the-harm-that-data-do/. .

[190] *Prygodicz vs. Commonwealth of Australia*, Federal Court of Australia 634, No. 2, ¶7 (2021).

[191] Joanna Redden, "The Harm that Data Do: Paying Attention to How Algorithmic Systems Impact Marginalized People Worldwide is Key to a Just and Equitable Future", SCIENTIFIC AMERICAN, (1 NOV. 2018), https://www.scientificamerican.com/article/the-harm-that-data-do/.

of robodebt, and in 2021, a federal court approved a settlement.[192] The government refunded hundreds of millions of Australian dollars in unlawfully collected debts and dropped claims for approximately one billion Australian dollars in false debts.[193] It was recently announced that the Royal Commission will conduct an investigation into the system, with a report to be issued in April, 2023.[194]

While the class action challenged robodebt on the basis that the government had unjustly enriched itself,[195] numerous stories shared in the media illustrated how the automated system had violated beneficiaries' rights, including their human rights. DHS's use of robodebt undermined eligible peoples' ability to provide for their families and themselves and operated without a navigable process for redress. In some cases, suicides by former social security beneficiaries were alleged to be the result of its harms.[196] Reliance on similar automated public benefits systems, if conducted by a party to the ECHR and producing similar harms, could potentially constitute violations of ECHR Article 8, insofar as they may interfere in family life[197] by preventing people already disadvantaged — by poverty, financial precarity, and in many cases disability — from providing for their families' basic material needs.

2) Colombia's Sisben Digitized Social Security System

The Serbian Social Card Law's exclusionary purposes and lack of adherence to data protection principles including transparency, contestability, data minimization, and accuracy recall problematic elements of Colombia's "Sisben" digital social welfare information system.

Colombia's Sisben information system, intended to administer its welfare policies, stands for System of Possible Beneficiaries of Social Programs. It was created in the 1990s with the main purpose of identifying, classifying and organizing in an easy, objective, and rapid way vulnerable and poor individuals who may become beneficiaries of national-wide social benefits.[198]

---

[192] "Robodebt Class Action: Federal Court has approved Robodebt settlement", Gordon Legal, Robodebt Class Action Settlement, available at https://gordonlegal.com.au/robodebt-class-action/.

[193] "Robodebt Class Action: Federal Court has approved Robodebt settlement: Key Points of Robodebt Class Action", Gordon Legal, Robodebt Class Action Settlement, available at https://gordonlegal.com.au/robodebt-class-action/.

[194] Australia to hold wide-ranging inquiry into automated debt recovery scheme, REUTERS (25 August 2022), https://www.reuters.com/world/asia-pacific/australia-hold-wide-ranging-inquiry-into-automated-debt-recovery-scheme-2022-08-25/.

[195] *Prygodicz vs. Commonwealth of Australia*, Federal Court of Australia 634, No. 2, ¶3(a) (2021).

[196] "Judge criticises government for allegedly refusing to tell grieving mother about son's robodebt", THE GUARDIAN (6 May 2021), https://www.theguardian.com/australia-news/2021/may/06/judge-criticises-government-for-allegedly-refusing-to-tell-grieving-mother-about-sons-robodebt.

[197] *See* Saidoun and Fawsie vs. Greece, European Court of Human Rights, Nos. 40083/07 and 40080/07, ¶46 (2011), available at https://www.asylumlawdatabase.eu/sites/default/files/aldfiles/AFFAIRE%20Saidoun%20c.%20Grece.pdf (finding a violation of Article 8, when taken together with Article 14, where the state denied numerous-family benefits to petitioner's family, claiming that their lack of Greek or EU nationality excluded them from receiving this benefit).

[198] Departamento Administrativo de la Función Pública de la República de Colombia, Decreto 441 de 2017 "Por el cual se sustituye el Título 8 del Libro 2 de la Parte 2 del Decreto 1082 de 2015, Decreto Único Reglamentario del Sector Administrativo de Planeación Nacional, con el fin de reglamentar el artículo 24 de la Ley 1176 de 2007 respecto del instrumento de focalización de los servicios sociales, y se dictan otras disposiciones", available at: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=80193.

As any information system, Sisben has had multiple updates. The most recent one, Sisben IV, changed the criteria by which people are classified according to their vulnerabilities.[199] This last update also introduced incontestable and opaque technology that relied on cross-referencing data from different official and private databases.

Previously, potential beneficiaries were scored from 0 to 100 based on multiple in-depth interviews that allowed the State to calculate the level of vulnerability each person was experiencing—according to a list of have and have-nots.[200]

The most recent update categorized potential beneficiaries into four main categories: (extreme poverty; moderate poverty; vulnerable; not poor nor vulnerable) based not on scoring but on predicting vulnerability according to an estimation of the future income that the potential beneficiary would be able to produce and obtain.[201] So, according to the new criteria, the less vulnerable are those who are still able to contribute to the household's finances, as determined by the prediction of an algorithm. This new focus has many problems.

First, information related to the algorithm is confidential: how it works, how it was designed, and according to what criteria or how it makes its predictions. Fundación Karisma, a Colombian civil society organization that conducted research on the issue, asked for details on the technology involved. The public entity in charge of Sisben, the National Development Office (NDO) has not provided information on how the algorithm calculates criteria, alleging the need to avoid fraud that could supposedly be unleashed if the government informed how the algorithm works.[202]

Second, the new system cross-references multiple databases of public and private nature (a total of 34), according to information provided by the NDO. Most of the databases have information of a sensitive nature, and any inconsistency on the data about the potential beneficiary can be used as a justification to deny him/her a social benefit.[203]

The last update of the criteria adopted by Sisben includes the exclusion of fraudulent beneficiaries. It has its roots in inconsistencies in the public statistics which suggested that by 2016, the number of vulnerable people was decreasing, while social benefits were being granted to a larger group of people.[204] However, the response to that reality was to introduce a policy of exclusion of those with

---

[199] Consejo Nacional de Política Económica y Social de la República de Colombia, Departamento Nacional de Planeación, Declaración de la Importancia Estratégica de Identificación de Potenciales Beneficiarios (Sisbén IV), 5 December 2016, pp. 34-37, available at https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3877.pdf.

[200] *Id.* at 16.

[201] *Id.* at 21; *See also* Joan López, *Experimentando con la pobreza: El Sisbén y los proyectos de analítica de datos en Colombia,* Fundación Karisma (2020), 11-13, https://web.karisma.org.co/wp-content/uploads/download-manager-files/Experimentando%20con%20la%20pobreza.pdf.

[202] *Id.* at 13 (citing "Respuesta solicitud de información Rad. 20196000094942, Departamento Nacional de Planeación–DNP. (2019)). *See also* Joan López, "¡La suerte está echada! Los merecedores deben ser elegidos por sus posibles ingresos y no por lo que tienen", (20 February 2020), Fundación Karisma, https://web.karisma.org.co/la-suerte-esta-echada-los-merecedores-deben-ser-elegidos-por-sus-posibles-ingresos-y-no-por-lo-que-tienen/.

[203] "¡No pueden ser tantos pobres! La exclusión de personas beneficiarias del sisbén a través de analítica de datos", Fundación Karisma, (20 Feb. 2020), https://web.karisma.org.co/no-pueden-ser-tantos-pobres-la-exclusion-de-personas-beneficiarias-del-sisben-a-traves-de-analitica-de-datos/

[204] In 2016, the head of the DNP stated, "Of all the modalities of fraud, it is extremely outrageous that this is happening, it is social theft, it is supremely unfair to the humblest Colombians. The problem with letting high-income Colombians

capacity to obtain an income in the long term, resulting in the exclusion of hundreds of former beneficiaries that can still be in a situation of poverty or vulnerability, along with the impossibility of the excluded to challenge those decisions.

Though fraud is the exception, the response from the NDO was to deploy a new criterion, reinforced by a technology, that turns potential beneficiaries into suspects of fraud and may exclude beneficiaries that might still be in a situation of poverty or vulnerability. Under the new system, people do not fully understand why they were excluded, and the government has not provided a special mechanism to challenge unfair decisions or ask for a review of their own cases.[205]

This case calls attention to how technologies are being deployed without enough scrutiny and accountability.[206] When large amounts of information are used to support vital decisions on who deserves to be a beneficiary of social protection policies, there should be stronger measures in terms of accountability, transparency and access to an effective remedy when the decision taken has no grounds or has been arbitrary. Second, automation in processes related to the social protection programs can result in arbitrariness and must be met with accountability, redress, transparency and explicability measures, with the transparency of the system being the rule. Third, people should not be punished by inconsistencies found in their data. States have a duty to keep data and people's records up to date, and people should be given an opportunity to contribute to that effort. But when an inconsistency on multiple data points is found, it should not trump human rights, such as due process or the presumption of innocence. An inconsistency is not *per se* an indicator of deliberate fraud, but a common result of previous decentralized databases administered by different third parties, something that may surface only when centralization measures are carried out. When inconsistencies are to be expected the population should be given a reasonable time to contribute with the updating efforts that should be widely informed. As a result of these problems, this system has been the subject of many lawsuits.[207]

3) India's Aadhaar Computerized System

The concerns noted in relation to the Social Card law's treatment of data security, accuracy, contestability, privacy, and potential for arbitrary or discriminatory exclusions are similar to issues associated with the Aadhaar unique identification system in India, which was first introduced in 2008.

The stated purpose of this system is to register all citizens and legal residents of India and to provide each person with a unique identification number and biometric profile. Since its introduction Aadhaar

---

achieve low Sisbén scores is that they cut in line and take the job away from a low-income person who genuinely needs it.". Cfr. "DNP alerta por nuevos 'colados' en el sisbén que ganan $3,8 millones al mes", Departamento Nacional de Planeación, (13 October 2016), https://www.dnp.gov.co/Paginas/DNP-alerta-por-nuevos-%E2%80%98colados%E2%80%99-en-el-Sisb%C3%A9n.aspx

205 Joan López, "¡La suerte está echada! Los merecedores deben ser elegidos por sus posibles ingresos y no por lo que tienen", (20 February 2020), Fundación Karisma, https://web.karisma.org.co/la-suerte-esta-echada-los-merecedores-deben-ser-elegidos-por-sus-posibles-ingresos-y-no-por-lo-que-tienen/. In fact, the Colombian Constitutional Court has decided diverse cases recognizing how hard it is for beneficiaries to update their personal data on Sisben in order to obtain a new evaluation of their vulnerable condition. *See* Corte Constitucional de Colombia, Judgement T-270/20, 31 Jul. 2020, available at: https://www.corteconstitucional.gov.co/relatoria/2020/T-270-20.htm.

206 Center for Human Rights and Global Justice, *Chosen by the Secret Algorithm: Colombia's Top-Down Pandemic Payments,* New York School of Law, (2021), https://www.youtube.com/watch?v=9MKm79iJ3X4.

207 *Id.*

has been used as a way of verifying and authenticating identity information across many public services, including social security benefits, food rations, fuel subsidies, and education, using wholly digitalized methods. However, this system has led to the exclusion of millions from social benefits, persistent issues with data quality, and worrying breaches of data security.

Much like the Social Card Law, one of the justifications for Aadhaar was to increase efficiency and inclusion in public services. However, over a decade of experience has demonstrated that the system has led to significant exclusion of otherwise eligible beneficiaries from fundamental social services. Several independent audits and studies have identified significant error rates, duplications in biometric profiles, and significant costs.[208] One 2018 report found that in just three Indian states, nearly two million people were excluded from access to food subsidies as a result of Aadhaar-related factors.[209] A follow up report in 2019 found that an estimated 4 million people had experienced exclusion from at least one service as a result of Aadhaar-related issues.[210] Further independent evaluations have demonstrated that linking Aadhaar with the welfare system has failed to achieve stated purposes such as increasing exclusion, reducing fraud and corruption or generating efficiency savings.[211] A further issue is that the grievance redress system is difficult to navigate and is dependent on individuals having access to a mobile phone.[212]

Furthermore, the system has presented significant cybersecurity risks. A report by the Center for Internet and Society (CIS) revealed that the Indian government inadvertently published the biographic and demographic data linked with Aadhaar numbers on 135 million Indians on the open internet.[213] This is in addition to serious breaches of personal data and privacy that had already resulted from security breaches in the Aadhaar system:

(a) for $8, it was possible to obtain an administrator access code to access the information of 1.2 billion Indians integrated into the system[214];
(b) in May 2017, a large-scale cyberattack targeting the network compromised the data of 130 million people, now accessible on the dark web.[215]

---

[208] Ronald Abraham, State of Aadhar Report 2017-2018, IDinsight, (2018), pp. 1 available at https://stateofaadhaar.in/assets/download/State_of_Aadhaar_Report_2017-18.pdf; Comptroller and Auditor General of India, Performance Audit Report NO. 24 of 2021 on 'Functioning of Unique Identification Authority of India', 6 April 2022, available at https://cag.gov.in/webroot/uploads/download_audit_report/2021/24%20of%202021_UIDAI-0624d8136a02d72.65885742.pdf.

[209] Ronald Abraham, State of Aadhar Report 2017-2018, IDinsight, (2018), pp. 24.

[210] Ronald Abraham, State of Aadhar Report 2017-2018, IDinsight, (2018).

[211] Reetika Khera, *Impact of Aadhar in Welfare Programmes*, Indian Institute of Technology Delhi, (2017), available at https://ssrn.com/abstract=3045235; Reetika Khern, "Why India's Big Fix is a Big Flub," NEW YORK TIMES, (21 January, 2018), https://www.nytimes.com/2018/01/21/opinion/india-aadhar-biometric-id.html.

[212] Vyom Anil and Jean Dreze, Wild Chase for Identity, The Indian Express, July 5, 2021.

[213] Amber Sinha and Srinivas Kodali, *Information Security Practices of Aadhar (or lack thereof): A documentation of Aadhar Numbers with sensitive personal financial information,* Centre for Internet & Society (2017), available at https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof/.

[214] "Investigation into biometric hacking of 1.2 billion Indians ", LE FIGARO (4 January 2018), https://www.lefigaro.fr/secteur/high-tech/2018/01/04/32001-20180104ARTFIG00264-enquete-sur-le-piratage-des-donnees-biometriques-de-12-milliard-d-indiens.php

[215] *Id.*

As a result of system failures, exclusion, and concerns about the right to privacy, Aadhaar is the subject of dozens of lawsuits in Indian courts. In a consequential decision before the Supreme Court of India in 2008, , the court recognized a fundamental right to privacy, and placed meaningful restrictions on the use of te Aadhaar system, including restricted private sector linkage of services to Aadhaar enrollment, greatly limited the mandatory use of Aadhaar for delivery of government services, permitted children to opt out of the system entirely until they turn 18, mandated an effective redress mechanism where data is misused, and further limited the kind of data the government is permitted to collect and for how long it can store authentication logs (reducing this period from 5 years to 6 months).[216]

The issues surrounding Aadhaar demonstrate some of the risks with using a centralized digital system to mediate access to a range of social benefits. It shows some of the difficulties for such a system to maintain accurate information across large groups of individual people, which necessarily leads to the exclusion of those who are unable to register or have errors in their digital records. Often those excluded would be those who belong to historically marginalized groups; for instance in India, the Aadhaar system has been used as a tool to exclude the muslim population in the state of Assam.[217] Furthermore, issues of data completeness, data quality, and data security often lead to risks of access to social security benefits, further compounding violations of rights. The profound effect of a lack of transparency and an accessible remedy should be key lessons for the Social Cards Law.

4) The United Kingdom's "Universal Credit" System

As the Social Card Law provides for automation within the benefits system in Serbia, the evidence of human rights violations and problems coming out of the United Kingdom's digitalized welfare system are of significant comparative value and warn against the adoption of such an approach.

One of the foundational components of the UK welfare system is a program named "Universal Credit," which provides a means-tested cash benefit for those on low incomes. The system relies on automated decision-making in: assessing and calculating the financial support to which an individual is entitled, authenticating individuals' identity, disbursing payments, determining debt recovery, and detecting fraud. Issues and exclusions have arisen from many of these automated processes,[218] but the automated calculation of the amounts to which individuals and couples are entitled has caused

---

[216] *Puttaswamy v. Union of India & Others*, Petition No. 494 of 2012, Supreme Court of India (26 September 2018), "Initial analysis of Indian Supreme Court decision on Aadhaar, Privacy International, (26 September 2018), https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar.

[217] This is currently the subject of a Supreme Court challenge, *see* Bikash Sing, "Assam to approach Supreme Court for providing Aadhar cards to NRC applicants", ECONOMIC TIMES (21 April 2022), https://m.economictimes.com/assam-to-approach-supreme-court-for-aadhaar-to-nrc-applicants/articleshow/90973922.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

[218] *See generally* Report of the Special Rapporteur on extreme poverty and human rights on Visit to the United Kingdom of Great Britain and Northern Ireland, 23 April 2019, A/HRC/41.39/Add. 1, available at https://digitallibrary.un.org/record/3806308?ln=en; Child Poverty Action Group, "Computer Says 'No!' Stage One: Information Provision", (2019) available at https://cpag.org.uk/policy-and-campaigns/report/computer-says-no-stage-one-information-provision; Rita Griffiths, "Universal Credit and Automated Decision Making: A Case of the Digital Tail Wagging the Policy Dog?", Social Policy and Society (2021) 1-18; Bryan Glick, "Thousands of Universal Credit claimants unable to use Gov.Uk Verify to apply for benefits," COMPUTER WEEKLY, (31 January 2018), https://www.computerweekly.com/news/252434188/Thousands-of-Universal-Credit-claimants-unable-to-use-Govuk-Verify-to-apply-for-benefits

particularly severe problems. To arrive at this calculation, data about beneficiaries' earnings from employment, communicated to the tax authority by employers, is transferred in bulk to the welfare authority on a regular basis. The welfare authority combines this income data with its own data about other income (such as pensions), and an automated assessment of the amount to which the individual is entitled is created accordingly. This automated system has created serious problems for some beneficiaries. For example, if an employer enters incorrect information about their employee's wages, accidentally inputting much higher earnings than the individual really received, the individual suffers: her payments are automatically stopped because her income has purportedly exceeded the relevant threshold. The beneficiary is then left without payments at all. Where errors are made which result in the automated system *overpaying* beneficiaries, this also causes serious problems as beneficiaries are then forced to repay any overpayments. This also occurs through an automated system. As overpayments are automatically deducted from beneficiaries' future payments, their future welfare payments are therefore lower than they otherwise would be, and they are left with very little to live on.[219] The UK's largest foodbank network has found that these kinds of errors and automatic repayment processes are the most persistent issues faced by the welfare claimants it assists with food parcels.[220]

The harms caused by the automated processes at the heart of Universal Credit benefits calculations were brought to the fore in *Secretary of State for Work and Pensions v Danielle Johnson & Ors,*[221] a case concerning a mismatch between automated decision-making and the realities of individuals' lives, in which approximately 85,000 individuals were affected. Under Universal Credit, claimants' income is assessed within a monthly assessment period: the amount to which a beneficiary is entitled each month is automatically calculated on the basis of the amount of money she has received within the previous month. But the design of the automated system did not account for the fact that, if a payday falls on a public holiday or weekend, wages are generally paid on a different day. Claimants would therefore sometimes receive two monthly salary payments within one monthly assessment period.[222] Where this happens, the Universal Credit system would automatically adjust payments down in response to the beneficiary's apparently-high income that month and, when the beneficiary would then receive no monthly salary payment during the next monthly assessment period, the Universal Credit payment would be much higher. These fluctuations in payments are not only disruptive in themselves, making it very difficult for beneficiaries to budget and thereby leading them to incur additional debts and high interest on short term loans or unpaid bills. In addition, these fluctuations do not even themselves out

219 Child Poverty Action Group, "Computer Says 'No!' Stage One: Information Provision" (2019), pp. 13.

220 Abhaya Kitendra, *Left Behind: Is Universal Credit Truly Universal?,* The Trussell Trust (2018), pp. 3, available at https://s3-eu-west-1.amazonaws.com/trusselltrust-documents/Trussell-Trust-Left-Behind-2018.pdf

221 *Secretary of State for Work and Pensions vs. Danielle Johnson,* Court of Appeal (Civil Division) of the Royal Court of Justice, Case No. C1/2019/0593 (2020), available at chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cpag.org.uk/sites/default/files/files/C1.2019.0593-2020-EWCA-Civ-778-R-Johnson-and-others-v-SSWP-FINAL-for-HAND-DOWN.pdf

222 For example, if a claimant is paid on the last working day of the month, and her assessment period runs from the last day of the month to the penultimate day of the following month, then she would frequently experience this problem. During the assessment period from 28th February to 30th March 2018, she would be paid on 28th February and 29th March, because 30thh March 2018 is a public holiday (a "non-banking day"). Her next assessment period ends on 29 April, but she receives her next payment on 30 April. The beneficiary would therefore be paid twice within the first assessment period and not receive any payment in the second.

over time. The design of Universal Credit means that "claimants affected by this problem irrevocably lose money over the course of a year" - sometimes hundreds of pounds.[223]

The Court of Appeal described the oscillations in the payments disbursed through this automated system as "perverse", noting that they "cause considerable hardship," and finding that the irretrievable loss of benefits to which beneficiaries would otherwise be entitled were it not for the mismatch to be "the most egregious aspect of the way the system works."[224] Particularly in light of the size of the cohort affected (tens of thousands), the duration of the impact on them (continuous, with no way for claimants to fix the problem themselves), and "the arbitrary nature of the problem", the Court of Appeal found that the government's failure to address the problem was unlawful.

Other cases concerning the Universal Credit system have also found violations of human rights law. In several cases, the High Court and Court of Appeal have found that welfare beneficiaries' rights under Article 14 of the European Convention on Human Rights were violated.[225] Courts have on several occasions found that, when severely disabled beneficiaries transitioned from the old social security system to the Universal Credit system and were left with lower payments, they had been unlawfully discriminated against.

5) Kenya's National Integrated Identity Management System

The perils, vulnerabilities, and propensities for unchecked errors and unfairness of a large-scale centralized sensitive digital data collection system without adequate safeguards—of the kind envisioned in the Social Card Law—is demonstrated by the example of the National Integrated Identity Management System (NIIMS) in Kenya.

The 2019 amendments to The Registration of Persons Act, Cap 107 of 1947 granted the Kenyan State extreme powers to collect personal information for the purposes of establishing NIIMS. The goal of NIIMS was to create a single centralized system for the identification of a person, contained in a unique identity number (Huduma Namba).[226] To complete the single register, the government commanded that Kenyan citizens and foreign nationals (including refugees and stateless persons) submit to authorities sensitive personal information purportedly to establish, verify and authenticate their identity, mainly through a mass campaign of collecting biometric data through fingerprinting.[227]

This operation's technical specifications and planned practical implementation remained opaque, with inadequate and conflicting information provided to the public. The legislative amendments placed no

---

[223] *Secretary of State for Work and Pensions vs. Danielle Johnson,* Court of Appeal (Civil Division) of the Royal Court of Justice, Case No. C1/2019/0593 (2020), ¶¶ 3, 60.

[224] *Id.* at ¶¶59, 62.

[225] See On the Application Of TP, AR, AB & F vs. Secretary of State for Work and Pensions, High Court of Justice, (Administrative Court), Case No. CO/4187/2019, (2020) available at https://www.rightsnet.org.uk/pdfs/2022_EWHC_123_Admin.pdf; On the Application Of TP, AR, SXC vs. Secretary of State for Work and Pensions, Case No. C1/2018/1576 (2020), available at https://www.matrixlaw.co.uk/wp-content/uploads/2020/01/R-on-the-application-of-TP-AR-SXC-v-Secretary-of-State-for-Work-and-Pensions-2020-EWCA-Civ-37.pdf; On the Application Of TD, AD, and Reynolds vs. Secretary of State for Work and Pensions, Case No. C1/2019/0640 (2020), available at https://www.judiciary.uk/wp-content/uploads/2020/05/TD-and-Ors-v-SSWP-judgment-Final.pdf

[226] Kenya: Statute Law (Miscellaneous Amendments) No. 18 (2018).

[227] *See generally* Registration of Persons Act No. 33 of 1947 (as amended to 2012), §3.

limits on the scope of data that could be captured and stored in the NIIMS database. For instance, the database was to be linked with other official registries in order to deliver an undefined sphere of government services (including: access to identification documents, universal healthcare, fertilizer subsidies, cash transfers, affordable housing and education).[228] Additionally, the Registration of Persons Act also supported the centralization of all production of identity credentials, including national identity cards, birth and death certificates, work permits and passports.

Kenyans faced potentially numerous problems with this single register system. First, there were no clear guidelines on who would have access to the data. Additionally, no clear protections were in place to ensure that unauthorized people with ill motives would be barred from gaining access to use one's data to take their benefits.[229] Third, the law failed to specify procedures for rectifying data that was incorrectly gathered or stored about someone. As such, individuals could be excluded or left out for lack of matching data.[230]

The nature of the NIIMS system—serving as the only reference source for a person's identity– makes it possible to model individual behavioral patterns and implement mass surveillance. The database is designed to contain information from all Kenyans and foreigners residing in Kenya and will serve as a reference point to facilitate access to the country's services.[231] Metadata about when a person interacts with the system—i.e. uses their Huduma card to access a service—with *Huduma Namba-related* services can be saved indefinitely and accessible within a single system. The NIIMS system, which is designed to record all the interactions of the Kenyan population, will therefore be able to establish the profile of these individuals.

Prior to NIIMS, a similar project was planned by Kenya: the *Integrated Population Registry Service* (IPRS). The IPRS was also presented as a central database serving as the sole source of truth for the authentication of Kenyans for access to government services. However, risks in terms of personal data and the use of biometric systems had already been raised publicly in 2014 by the NGO Privacy International concerning the Kenyan IPRS project,[232] and in particular:

- the misappropriation of data and its fraudulent use;
- errors in the identification of a person;
- a system that is not exempt from exclusion, with the example of the failure to recognize the footprints of plowmen and dark-skinned individuals;

---

[228] Amber Sinha, *Governing ID: Kenya's Huduma Namba Programme,* The Centre for Internet & Society, (2020, pp. 4 ("The Huduma Namba is clearly intended to serve as a foundational and single identity system to which all other government databases shall be linked.")

[229] Amber Sinha, *Governing ID: Kenya's Huduma Namba Programme,* The Centre for Internet & Society, (2020, pp. 6. There are multiple ways in which unauthorized persons may use someone else's data, including for identity theft purposes, phishing, targeted advertising, or other, more dangerous forms of targeting and harassment.

[230] *Id.*

[231] Official website of Huduma Namba: https://www.hudumanamba.go.ke. In the original version, the mission statement reads: "to create and manage a central master population database which will be the 'single source of truth' on a person's identity. The database will contain information of all Kenyan citizens and foreign nationals residing in Kenya and will serve as a reference point for ease of service delivery to the people of Kenya".

[232] Privacy International and National Coalition of Human Rights Defenders in Kenya, *The Right to Privacy in Kenya* (2014), pp. 11-12, available at https://privacyinternational.org/sites/default/files/2017-12/UPR%20Kenya.pdf.

- the unregulated retention of biometric data, raising the risk of their use for a use other than that initially intended, and more generally the risk of data theft.

In addition, the NIIMS contract between IDEMIA and Kenya was concluded when the country had no legislation on the protection of personal data. It was only in 2019 that Kenya adopted a *Data Protection Act*.

In this regard, the High Court of Kenya ruled that the *Data Protection Act* should have been passed before the NIIMs Act was passed and before the collection and processing of personal data from this project.[233] The same court also ruled in October 2021 that a data protection impact assessment must be carried out by the authorities before the operationalisation of NIIMS.[234] This analysis, provided for by the *Data Protection Act*, aims to assess the risks posed by the system to the rights and freedoms of the individuals whose data is processed, and to establish the appropriate measures and guarantees to ensure the protection of this data.[235] At present, the operational implementation of the NIIMS system has been suspended by this judgment of October 2021, pending the results of the impact study. Other legal proceedings concerning NIIMS are also pending.

The NIIMS system created great fears. The NIIMS system involved multiple stages that could lead to discrimination and exclusion of certain parts of the population, particularly because of their ethnic origin or status (refugees and stateless persons).[236] Its use by the authorities could allow the continuation of this discrimination and thus infringe the right to equality. An erroneous registration designating the person as a foreigner can be used as a tool for deliberate exclusion. This risk is particularly high in countries with a history of ethnic conflict, such as Kenya.[237] NIIMS would not only facilitate the identification of members of certain communities on the basis of patterns that can be identified by analyzing their metadata, but it would also allow the government to put certain communities at increased risk of not being recognized as Kenyan. In fact, in the field, the absence of a birth certificate or identity card has resulted in many people refusing to register. Since the Kenyan government had indicated its intention to make the use of the NIIMS system mandatory for all residents to access these services, the impact of not being able to access these services became exacerbated.

6) The Netherlands' System Risk Indication Social Security Algorithm

---

233 "Data Protection Impact Assessment and ID Systems: the 2021 Kenyan ruling on Huduma Namba", Privacy International, (27 January 2022), *Nubian Rights Forum, https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma*.

234 *Republic vs. Joe Mucheru*, High Court of Kenya in Nairobi, Application No. E1138 of 2020, Judgment of 14 October 2021, ¶ 119, available on http://kenyalaw.org/caselaw/cases/view/220495/.

235 *See Data Protection Act* of 2019 for the Data protection impact assessment provided for in Article 31, available at http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019.

236 "Submission to the Office of the United Nations High Commissioner for Human Rights on the Impact of Digital Technologies on Social Protection and Human Rights", Amnesty International (2020), available at https://www.ohchr.org/sites/default/files/Documents/Issues/Poverty/DigitalTechnology/AmnestyInternational.pdf.

237 Following the terrorist attack on the Westgate Shopping Mall in Kenya in 2014, authorities rounded up detained them at a football stadium and verified their identity documents. Those who could not prove their citizenship were deported to Somalia. *See* "Kenya: Halt Crackdown on Somalis – Thousands arrested, nearly a hundred deportees", Human Rights Watch, (April 11, 2014), available at https://www.hrw.org/news/2014/04/11/kenya-halt-crackdown-somalis.

The Netherlands provides a key example of effective judicial review of a digitalized welfare system according to human rights law. A law providing for developments reminiscent of the Social Card Law system, whereby the Dutch government had sought to consolidate wide-ranging data about welfare beneficiaries and introduced automated systems into welfare programs, was struck down on human rights grounds. This is of direct relevance to the present case.

The System Risk Indication (SyRI) was an algorithm-based government system used by Dutch public bodies to identify those most likely to commit social security fraud. Legislation providing for this system allowed government agencies to process personal data from across government departments on the basis of categories such as gender, employment history, taxes, property ownership, education, health insurance, government permits, social assistance benefits, and to develop 'risk models' accordingly, in order to single out individuals worthy of investigation.[238] Risk profiles were shared between different public authorities, but individuals were unaware that these profiles existed. SyRI was not used evenly across the Netherlands, rather, it was deployed exclusively in neighborhoods with high numbers of low-income households.[239]

In 2020, the District Court of the Hague ruled that the SyRI legislation did not strike a fair balance between the social interest the legislation served (combating fraud in the interest of economic welfare) and the rights to private and family life of the individuals affected by the legislation.[240] According to the court, the system had a significant impact on the lives of people whose data was being processed, without sufficient protections to justify this interference.[241] The court also ruled that the SyRI legislation did not contain sufficient privacy safeguards and was "insufficiently transparent and verifiable."[242]

Further, the court agreed with the argument of the claimants and of the UN Special Rapporteur on extreme poverty and human rights that SyRI "has a discriminatory and stigmatizing effect" because it was deployed only in low-income neighborhoods.[243] The court noted: there "is in fact a risk that SyRI inadvertently creates links based on bias, such as a lower socio-economic status or an immigration background."[244]

The court based its decision on Article 8 (right to family life) of the European Convention on Human Rights and the principles of the General Data Protection Regulation effective in the European Union, which include transparency, purpose limitation, data minimization, accuracy, integrity, confidentiality, and accountability.[245] The legislation providing for SyRI was struck down, and the government halted its use of the system.

---

[238] Netherlands Juristen Comité voor de Mensenrechten et al. vs. The Netherlands, ECLI:NL:RBDHA, (2020), ¶6.51, at: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878

[239] *See* Brief by the United Nations Special Rapporteur on extreme poverty and human rights as Amicus Curiae in the case of NJCM c.s./De Staat der Nederlanden (SyRI) before the District Court of the Hague (case number C/09/550982/HAZA 18/388), available at https://www.ohchr.org/sites/default/files/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf

[240] *Id.* at ¶6.7

[241] *Id.* at ¶6.59.

[242] *Id.* at ¶6.7

[243] *Id.* at ¶6.92.

[244] *Id.* at ¶6.93.

[245] *See generally* Netherlands Juristen Comité voor de Mensenrechten et al. v. The Netherlands (2020).

7) Poland's Jobseeker Algorithmic Profiling System

The Polish profiling system of jobseekers was abolished following a Constitutional Court finding it unlawful, another example of judicial review stepping in to curtail algorithmic "black box" social welfare decision making of the kind the Social Card Law risks implementing.

In 2014, the Polish government introduced a profiling mechanism to determine the type of support a jobseeker would get from the public employment centers (Publiczne Służby Zatrudnienia - PSZ). The system was introduced to rationalize the use of public resources available, reduce bureaucratic inefficiency and result in better value for money. The system divided unemployed people into three groups, depending on how close they are to finding a job, by assigning them a score.

In 2016, a local nongovernmental organization, Panoptykon, asked the government to provide information on the criteria used by the algorithm to make assessments. Since the competent ministry did not provide an answer, the NGO recurred to the Warsaw Regional Administrative Court. The court found that the information is of public interest and that the authority had to provide information. Only at that point the Minister provided the list of data points used to calculate the scoring. The 24 data points include data on their age, gender, disability, and duration of employment.[246] Each group would then get a different level of support from the PSZ. The mechanism did not trigger an automated decision but was instead just meant to "advise" public officers who would ultimately make the decision. However, it was found that the mechanism hugely influenced their decision, as the "advice" of the algorithm was overridden in only 1 in 100 cases.[247]

Another point of concern was that data subjects were not able to correct information stored in the system.

The Supreme Audit Office (Najwyższa Izba Kontroli) assessed the profiling mechanism and concluded that it was ineffective and discriminatory. Under the scoring rules, people belonging to the most vulnerable segments of society (single mothers, people with disabilities, and rural residents) were more likely to receive less assistance. A survey among the employment agency's staff found that "44% of local job centers confirm that profiling is useless in their day-to-day work. And 80% conclude that the system should be changed."[248]

The Polish Ombudsman referred the case to the Constitutional Court which in 2018, found it unconstitutional and ordered the government to amend it in accordance with the Constitution. Following the court decision and the wide ranging criticism, the system was ultimately abolished in 2019.[249]

---

[246] Jędrzej Niklas, Karolina Sztandar-Sztanderska, Katarzyna Szymielewicz, *Profiling the Unemployed in Poland: Social and Political Implications of Algorithmic Decision Making*, Fundacja Panoptykon (2015), pp. 1, 37, available at https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf

[247] Jędrzej Niklas, *Poland: Government to scrap controversial unemployment scoring system*, ALGORITHMIC WATCH, (16 April 2019), https://algorithmwatch.org/en/poland-government-to-scrap-controversial-unemployment-scoring-system/

[248] *Id.*

[249] *Id.*

8) Uganda's Digital National Identification System

The discriminatory exclusions produced by the inaccessibility of the Ugandan national digital identification (ID) system, borne most heavily by historically marginalized groups—serve as a warning of some of the kinds of discrimination that will result from the Social Card Law, disproportionately harming Roma communities. In particular, the experience using the national ID as a means of accessing social rights in Uganda demonstrate the difficulties in ensuring access to a new digital system, how a digitalized system may replicate and exacerbate existing patterns of exclusion and discrimination within a given country, and how an opaque system may lead to severe, disproportionate, consequences for human rights.

Mass exclusion plagues the Ugandan national digital ID system. The national ID currently blocks many individuals' access to their lifesaving rights to health and social security, as well as other social rights. This impact is felt most acutely by already marginalized groups— including older persons, women, persons with disabilities, persons belonging to ethnic minority groups, persons whose Ugandan nationality is called into doubt by authorities, and those living in extreme poverty. This mass exclusion represents a serious human rights crisis in Uganda.

Uganda's national digital ID system with biometric components, *Ndaga Muntu*, was introduced in 2014, and the Registration of Persons' Act (ROPA) passed by the Ugandan Parliament in 2015 to provide a legal framework for the system. The digital ID system in Uganda consists of three main components: the national identity register (NIR), the national identity card (NIC), and the national identity number (NIN). Section 65 of ROPA establishes that the use of information in the NIR "shall be used" for a wide range of purposes, including "public administration" and "providing social services, including social security services, health, education, and welfare benefits." ROPA further provides in Section 66 for "Mandatory use of national identification cards," stating that "any ministry department or agency of government or any other institution providing a public service shall require a person accessing the service to produce a national identification number or national identification card or alien's identification number or alien's identification card." Section 66 enumerates a different list of services than Section 65, but includes "pension and social security transactions," and affords the government discretion to apply the provision to "any other purpose as may be prescribed by the Minister."

According to a report released in June 2021—*Chased Away and Left to Die: How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons*[250]—it was estimated that between 23 and 33% of the adult population had not yet received their national ID card.[251] This figure was later confirmed by current Executive Director of the National Identification and Registration Authority (NIRA), Rosemary Kisembo, during a session of ID4Africa on November 17, 2021.[252]

Despite the fact that numerous Ugandans do not have a national ID, it has become mandatory to access the right to health and social security and does not accept persons furnishing alternative forms

---

[250] Initiative for Social and Economic Rights, Center for Human Rights and Global Justice, Unwanted Witness, *Chased Away and Left to Die: How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons,*, Joint Report, (2021) available at: https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf.

[251] *Id.* at 9.

[252] ID4Africa, The Dark Side of Digital ID: Mitigating the Risks (Pt. 1), November 17, 2021, https://www.youtube.com/watch?v=oHKxo-walUk&t=7144s.

of identity enumerated under in the Registration of Persons Act, 2015 (ROPA).[253] The result is that, by the government's own calculations, millions of people in Uganda are currently barred from accessing lifesaving social rights. Some of those most affected by this exclusion are older persons, women, persons with disabilities, persons belonging to ethnic minorities, persons whose Ugandan nationality is questioned by authorities and those living in extreme poverty.

The Minister for Health (MoH) and the Minister for Gender, Labour & Social Development (MGLSD) began to integrate the digital ID into certain aspects of public service delivery. The integration in health care has thus far been limited to a requirement to present a national ID card or number when seeking access to some health services. Meanwhile, MGLSD has also integrated the national digital ID system in its Social Assistance Grants for Empowerment (SAGE) programme, which delivers cash transfers to older persons over the age of 80 through the Senior Citizens' Grant (SCG). This integration includes i) using the NIR as the sole means of identifying beneficiaries by their date of birth, ii) requiring individuals to present either a NIC or NIN for use by program administrators and Payment Service Providers (PSPs), and iii) requiring individuals to biometrically authenticate their identity in order to enroll and receive payments.

The existence of financial, administrative, legal, technological, and physical barriers erected in the context of digital ID systems, prevent certain groups from accessing the ID system and the human rights that become contingent on having an ID.

According to the Ministry of Gender, Labour & Social Development (MGLSD) at least 10,000 eligible older persons cannot access the Senior Citizens' Grant (a cash transfer program for older persons over 80 years) because they had been unable to register for a national ID, and a further 40,000 persons over 80 years of age had been wrongly excluded because of errors in the age listed on their national ID card; this represents almost a quarter of older persons over the age of 80 in Uganda.[254] Additionally, pregnant women were being denied treatment and turned away at public healthcare centers, even while in distress and bleeding, the result of a policy to refuse public health care to those without a national ID. This exclusion is therefore a life and death matter for many people in Uganda.

The National Identification Registration Authority (NIRA) is unable to bridge the significant identification gap. According to the Committee on Defence and Internal Affairs of the Ugandan Parliament, of 29 million people who had registered, as many as 10 million Ugandans who had registered had still not received their card.[255] These numbers suggest that while there has been some progress in registering more people, there is even slower progress issuing new cards.[256] This lack of progress is no doubt due to understaffing and often non-existent NIRA offices; the need for individuals to travel and incur significant costs in order to register, pick their card, or correct errors;

---

[253] The ROPA provides defines identity documents to include; a) birth certificate (b) baptism certificate; (c) immunization card; (d) a voter's identification card; (e) an immigration document; (f) a valid Uganda or foreign passport or a document that may be used in place of a passport; (g) a valid driving license; (h) a valid residence permit; or (i) a certificate of acquired citizenship.

[254] Initiative for Social and Economic Rights, Center for Human Rights and Global Justice, Unwanted Witness, *Chased Away and Left to Die: How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons,*, Joint Report, (June 8, 2021) pp. 42, available at: https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf.

[255] Franklin Draku, "Outdated NIRA machines leave 10m Ugandans without IDs," DAILY MONITOR (Uganda) (October 21, 2021) https://www.monitor.co.ug/uganda/news/national/outdated-nira-machines-leave-10m-ugandans-without-ids-3590632.

[256] *Id.*

slow processing times at headquarters; and the need to manually transport both data and cards between Kampala and every region of Uganda.[257]

According to Rosemary Kisembo, Executive Director of NIRA, the agency faces a budget shortfall—and that the technology procured from a German company in 2010 and 2014 to produce ID cards is now obsolete, making it impossible to obtain replacement parts. Furthermore, she revealed that the digital system behind the national ID was no longer being regularly updated, leaving it vulnerable to data breaches. Meanwhile, three of the four card printing machines Uganda has are now broken, leaving NIRA with the capacity to print only 1,000 cards per day; and there is apparently no budget to procure blank cards to print IDs.[258] NIRA officials blamed budget shortfalls, vendor lock-in, multiple registrations, as well as their inconvenient location on Kololo Ceremonial Grounds (where many events of state take place) for the delays.[259] But it is clear that regardless of the exact cause of the problem, no solution will be immediately forthcoming.

Despite NIRA being stuck in this stasis, the government has been continuing to enforce Section 66 of the Registration of Persons Act,[260] relying on the national ID as the exclusive (and mandatory) source of identification document for access to a variety of human rights. This has included access to public health services, access to the Senior Citizens' Grant, and access to COVID-19 vaccines. In March, 2020 civil society brought a suit against the government in March to prevent the national ID from being the only valid identity document in order to access the COVID-19 vaccine, triggering an almost immediate change in official policy,[261] Despite the Ministry of Health retracting its policy, community members have reported that many health workers continued to deny the vaccine to those who do not have a national ID.

On the Day of Older Persons on October 1, MPs made the welcome announcement that they wanted to lower the age of eligibility to the Senior Citizens' Grant (SCG). However, one MP recognized that "There is need to allow older persons to register with alternative identification documents because the National Identification cards have become so discriminatory"; it was reported that NIRA was currently overwhelmed because so many older persons were frantically trying to correct their date of birth as listed on their national ID card in order to enroll in the SCG.[262]

The fundamental problem remains: a significant part of the Ugandan population continues to be excluded from the national ID system, and therefore from access to critical human rights. It is helpful that government officials have acknowledged the severe challenges they face to make the digital ID system function properly. However, the days, weeks, months, and perhaps even years that it will take

---

[257] NATIONAL IDENTIFICATION AND REGISTRATION AUTHORITY (NIRA), Acceptance Speech of the Executive Director (May 30, 2021), pp. 2, available at https://www.nira.go.ug/about-nira/edz-message.

[258] "NIRA blames equipment challenges for delays in printing cards," NTV (October 20, 2021), https://www.youtube.com/watch?v=e6sgigpEPJw.

[259] *Id.*

[260] Registration of Persons Act, § 66, (2015), available at https://www.ugandalaws.com/principal-legislation/registration-of-persons-act#:~:text=An%20Act%20to%20harmonise%20and,identification%20cards%20and%20aliens%20identification.

[261] INITIATIVE FOR SOCIAL AND ECOMIC RIGHTS (ISER), Press Release on Ministry of Health's Withdrawal of National ID Requirement for Covid-19 Vaccine (March 10, 2021), https://iser-uganda.org/wp-content/uploads/2022/04/ISER_welcomes_MoH_withdrawal_of_National_ID_requirement_for_Covid_19_Vaccination.pdf/

[262] PARLIAMENT WATCH, MPs want SAGE eligibility age reduced (September 30, 2021), https://parliamentwatch.ug/news-amp-updates/mps-want-sage-eligibility-age-reduced/.

to fix the problems with the national ID will mean prolonged periods where marginalized individuals cannot access their right to health and social security; they continue to experience a form of 'social death.'[263] Yet the government has been unwilling to remove the requirement of the national ID to access these fundamental social rights.[264] Indeed, recent government emergency measures linking COVID-19 relief to the national ID and/or mobile phone ownership, which is contingent on having a national ID, confirms that this pattern of relying on the national ID as the exclusive source of identification is unlikely to stop without intervention.[265] This case is currently the subject of a legal challenge in the High Court of Kampala.[266]

V. Conclusion

In light of the foregoing, the author organizations submitting this brief to inform the consideration of the Serbian Constitutional Court affirm that the Serbian Social Card Law risks enabling serious and large-scale violations akin to those experienced in other jurisdictions where digitalization and social security have intersected. It is imperative as a matter of human rights implementation and precedent that the flaws noted in the legislation be remedied.

Sincerely,

Mandi Mudarikwa/Imogen Richmond-Bishop//Jelena Sesar
Amnesty International

Vivian Newman Pont
Centro de Estudios de Derecho, Justicia y Sociedad (Dejusticia)

Victoria Adelmant / Katelyn Cioffi
Digital Welfare State & Human Rights Project (DWS Project) based at the Center for Human Rights & Global Justice at New York University School of Law

Dorde Jovanovic
European Roma Rights Center (ERRC)

---

263 Franklin Draku, "Outdated NIRA machines leave 10m Ugandans without IDs," DAILY Monitor (Uganda) (October 21, 2021) https://www.monitor.co.ug/uganda/news/national/outdated-nira-machines-leave-10m-ugandans-without-ids-3590632.

264 NATIONAL IDENTIFICATION AND REGISTRATION AUTHORITY (NIRA), Acceptance Speech of the Executive Director (May 30, 2021), https://www.nira.go.ug/about-nira/edz-message.

265 "Mobile Money Cash for COVID-19 Poor," THE INDEPENDENT (UGANDA) (July 5, 2021), https://www.independent.co.ug/mobile-money-cash-for-covid-19-poor/; Dorothy Mukasa, Salima Namusobya, and Christiaan van Veen, "The Fatal Flaw in Uganda's Emergency Relief," AFRICAN ARGUMENTS (July 14, 2021), https://africanarguments.org/2021/07/the-fatal-flaw-in-ugandas-emergency-relief/.

266 Initiative for Social and Economic Rights, Unwanted Witness, and the Health Equity and Policy Initiative, Civil Society sues Government over Ndaga Muntu National ID: Mandatory Digital ID Threatens Lives, 25 April 2022, https://iser-uganda.org/wp-content/uploads/2022/07/Digital_ID_Litigation_Press_Statement.pdf.

Brian Alex Kiira
Initiative for Social and Economic Rights (ISER)

Davis Malombe
Kenya Human Rights Commission (KHRC)

Lucy Williams / Shannon Al-Wakeel
Program on Human Rights and the Global Economy (PHRGE) & Center for Public Interest Advocacy and Collaboration (CPIAC) at Northeastern University

Francesca Feruglio / María Eugenia Meléndez Margarida / Fernando Ribeiro Delgado
Secretariat of ESCR-Net - International Network for Economic, Social and Cultural Rights