ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

FOCUS HUMAN RIGHTS
14 OTTOBRE 2022

Digital Welfare State and Fundamental Rights: the Judicial Litigation on Digital Identification Systems in Kenya and Jamaica

by Giulia Formici
Research Fellow in Public Comparative Law
University of Milan

Digital Welfare State and Fundamental Rights: the Judicial Litigation on Digital Identification Systems in Kenya and Jamaica*

by Giulia Formici
Research Fellow in Public Comparative Law
University of Milan

Abstract [En]: Digital transformation of welfare states is expanding all over the world; notwithstanding the positive potentialities in terms of efficiency and cost savings, the implementation of digital tools poses serious challenges to the guarantee of fundamental rights. In this context, a significant case-study is represented by the creation of national biometric identification systems (BISs) with the purpose of providing unique digital identities required to access vital welfare services. While helping detecting frauds and guaranteeing a correct allocation of public resources, these automated instruments could ultimately affect not only privacy and data protection rights but also human dignity, non-discrimination and social rights by exacerbating existing social inequalities, to the detriment of disadvantaged and less 'digitally educated' segments of the population. The paper aims at analyzing, from a comparative perspective, these complex issues through the study of the most relevant judicial litigations on BISs in Jamaica and Kenya. This case-law ultimately imposes to seriously re-think a possible balance-point able to guarantee privacy and equality without renouncing to digitalization's potentialities.

Titolo: Welfare State digitale e diritti fondamentali: il contenzioso giudiziario sui sistemi di identificazione digitale in Kenya e Giamaica
Abstract [It]: La digitalizzazione del Welfare State è un fenomeno in continua espansione anche nei Paesi c.d. in via di sviluppo. Pur facendosi portatori di miglioramenti in termini di efficienza e contenimento della spesa pubblica, gli strumenti di Digital Welfare pongono tuttavia importanti sfide per la garanzia dei diritti fondamentali. Emblematico esempio del profondo dibattito sorto in tale contesto è rappresentato dall'utilizzo di sistemi di riconoscimento biometrico finalizzati all'attribuzione di una "identità digitale" unica e certa a cittadini e residenti nel territorio nazionale. Pur contribuendo ad una efficace allocazione delle risorse nonché alla lotta alle frodi, questi sistemi hanno provocato un significativo impatto non solo sui diritti alla privacy e alla protezione dei dati bensì sui diritti sociali, alla non discriminazione e alla dignità, esacerbando diseguaglianze e divari sociali. Il presente lavoro intende approfondire le rilevanti sfide poste dal Digital Welfare State attraverso l'analisi comparata di alcune importanti pronunce della Supreme Court giamaicana e della High Court kenyota aventi ad oggetto la legittimità e proporzionalità di sistemi di riconoscimento biometrico. Questi casi giurisprudenziali impongono di riflettere sulla urgenza di determinare un corretto bilanciamento tra potenzialità derivanti dalla digitalizzazione e tutela dei diritti fondamentali nel rapporto tra Stato e cittadini.

Keywords: Digital welfare state; social inequalities; Biometric Identification Systems; fundamental rights; digital identity; Jamaican Supreme Court; Kenyan High Court
Parole chiave: Digitalizzazione dei servizi di Welfare; diseguaglianze sociali; sistemi di riconoscimento biometrici; diritti fondamentali; identità digitale; Supreme Court giamaicana; High Court kenyota

* Articolo sottoposto a referaggio.

1. Datafying Welfare Services: The Fruit of Temptation

Big Data, algorithms, Artificial Intelligence (AI) and digitalization have become central in our vocabulary: these four words represent one of the biggest revolutions of our times and, at the same time, the most controversial technological advancements of the last decades. The unlimited spread of Internet and telecommunications opened the doors to a massive and unprecedented production of information: although there is not a generally accepted definition[1], the term 'Big Data' refers to the proliferation of data coming from a variety of sources (interactions on the Internet, online transactions, social networks, mobile apps, Internet of Things) and characterized by a gigantic volume of heterogeneous information. These data, considered the 'new oil' because of their enormous economic value[2], are collected, stored, retained, processed, and accessed thanks to sophisticated data analytics techniques: AI systems based on algorithms and trained using Big Data have revealed new horizons by increasing the ability to analyze and take advantage of the full value of data, especially when considered in their aggregated dimension[3].

The potentialities of these new technological tools are expressed in a wide range of sectors, from agriculture[4] to smart cities – where these instruments are employed to implement sustainable solutions and improve city life quality[5] –, from health[6] to pandemic emergency[7], from justice[8] to security[9].

[1] On Big Data and the difficulty to define this term, see, *ex multis*, J.S. WARD – A. BARKER, *Undefined by data: a survey on Big Data definitions*, arXiv Cornell University, 2013; B. VAN DER SLOOT – D. BROEDERS – E. SCHRIJVERS (eds), *Exploring the boundaries of Big Data*, Amsterdam, 2016; Y. MCDERMOTT, *Conceptualising the right to data protection in an era of Big Data*, in *Big Data & Society*, n. 1/2017.

[2] This emblematic expression has been used in THE ECONOMIST, *The world most valuable's resource is no longer oil, but data*, 6th May 2017; on the economic value of Big Data and Data Analytics, see P. VERHOEF – E. KOOGE – N. WALK, *Creating value with Big Data analytics*, London, 2016.

[3] See EUROPEAN PARLIAMENT, *Big data and data analytics. The potential for innovation and growth*, Briefing Paper, September 2016.

[4] K. BRONSON – I. KNEZEVIC, *Big Data in food and agriculture*, in *Big Data & Society*, n. 1/2016; M. TRIPOLI – J. SCHMIDHUBER, *Emerging opportunities for the application of blockchain in the agri-food industry*, FAO, 2018; J.P. BELAND *et al.*, *Big Data for agri-food 4.0: application to sustainability management for by-products supply chain*, in *Computers in Industry,* n. 1/2019.

[5] T. KIM – C. RAMOS – S. MOHAMMED, *Smart city and IoT*, Amsterdam, 2017; G.F. FERRARI, *Le smart cities al tempo della resilienza*, Sesto San Giovanni, 2022.

[6] M. RATH – B. PATTANAYAK, *Technological improvement in modern health care applications using IoT and proposal of novel health care approach*, in *International Journal of Human Rights in Healthcare*, n. 2/2019; M. SINISI, *Uso dei big data e principio di proporzionalità*, in *Federalismi.it. Osservatorio di diritto sanitario*, n. 8/2020; L. SCAFFARDI, *La medicina alla prova dell'Intelligenza Artificiale*, in *DPCE Online*, n. 1/2022.

[7] A. DUBOV *et al.*, *The value and ethics of using technology to contain the Covid-19 epidemic*, in *The American Journal of Bioethics*, n. 7/2020; A. GUINCHARD, *Our digital footprint under Covid-19: should we fear the digital contact tracing app?*, in *International Review of Law, Computers and Technology*, 15th July 2020.

[8] F. BEX *et al.*, *Special Issue on Artificial Intelligence for Justice*, in *Artificial Intelligence and Law*, n. 1-3/2017; L. VIOLA, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte,* in *Federalismi.it*, n. 21/2018; COUNCIL OF EUROPE, *European ethical charter on the use of AI in judicial systems and their environment*, 2018; C. CASONATO, *Intelligenza artificiale e giustizia: potenzialità e rischi*, in ***DPCE Online***, n. 3/2020; S. PENASA, *Intelligenza artificiale e giustizia: il delicato equilibrio tra affidabilità tecnologica e sostenibilità costituzionale in prospettiva comparata*, in *DPCE Online*, n. 1/2022.

[9] A.J. MCCLURG, *In the face of danger: facial recognition and the limits of privacy law*, in *Harvard Law Review*, n. 120/2007; H. RUHRMANN, *Facing the future: protecting human rights in policy strategies for facial recognition technology in law enforcement*, Berkeley, 2019; I. REZENDE, *Facial recognition in police hands: assessing the Clearview case from a European perspective*, in *New Journal of*

Moreover, in recent times, Governments have progressively applied technological innovations to promote efficiency in public services, including social protection and assistance systems which are more and more driven by digital technologies and automated systems[10].

In particular, digitalization and technological progress have become fundamental engines for the welfare states' evolution: particularly after the 2008 economic crisis and the consequent austerity policies, Governments and public administrations started a new path towards digital transition and automation[11] with the final purpose of strengthening impartiality and efficiency in decision-making, enhancing forms of control and preventing tax frauds, identity frauds, fraudulent claims and dysfunctions. The innovative instruments employed – among which digital identification systems, welfare benefits calculation systems, risk scoring classification or eligibility assessment tools[12] – have been considered fundamental allies to achieve a better management and a good governance of public resources, a correct allocation of funds, a reduction of economic waste and an increase in savings, especially in times of reduced resources. Automation has also been considered able to minimize the problematic phenomena of corruption and bias, by promoting more objective decisions and procedures[13]. For all these reasons, it comes with no surprise that the 'digital and automated (r)evolution' has significantly touched upon welfare services: "welfare is an attractive entry point [for new digitalized technologies] not just because it takes up a major share of the national budget or affects such a large proportion of the population but because digitization can be presented as an essentially benign initiative"[14].

Despite the declared beneficial effects and great potentialities, the global spread of what has been called 'digital welfare state' – meaning "systems of social protection and assistance increasingly driven by digital data and technologies"[15] – didn't come without great concerns. In fact, it hasn't been ignored how this

European Criminal Law, n. 3/2020; G. MOBILIO, *Tecnologie di riconoscimento facciale: rischi per i diritti fondamentali e sfide regolative*, Naples, 2021.

[10] In this Journal, see D-U. GALETTA – J. G. CORVALAN, *Intelligenza artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, n. 3/2019; C. BENETAZZO, *Intelligenza artificiale e nuove forme di interazione tra cittadino e pubblica amministrazione*, n. 16/2020; A. PAPA, *Intelligenza Artificiale e decisioni pubbliche tra tecnica, politica e tutela dei diritti*, n. 22/2022.

[11] Broadly on this point, M.R. BUSEMEYER – A. KEMMERLING – K. VAN KERSBERGEN – P. MARX (eds), *Digitalization and the Welfare State*, Oxford, 2022.

[12] For a brief survey of these instruments, see P. ALSTON, *Report of the Special Rapporteur on extreme poverty and human rights*, UN General Assembly, 11 October 2019 (A/74/493).

[13] See M. ZALNIERIUTE – L. BENNET MOSES – G. WILLIAMS, *The rule of law and automation of government decision-making*, in *The Modern Law Review*, n. 3/2019.

[14] P. ALSTON, *Report*, cit., p. 3. As similarly underlined by Bertolini, "welfare represents another sector where state deficiencies are more evident and thus the algorithm is considered be mostly needed", E. BERTOLINI, *Is technology really inclusive? Some suggestions from States run algorithmic programs*, in *Global Jurist*, 2020, p. 8.

[15] P. ALSTON, *Report*, cit., p 4. See also the definitions provided by the Digital Freedom Fund: "Digital system refers to any data-driven, digital or automated process used in the provision and policing of social protection, varying from identity verification, needs assessments, calculation and payment of benefits, and fraud detection. For the purpose of this strategy, the term 'digital systems' also extends to practices surrounding and leading up to the use of these systems; digital welfare state refers to the use of digital systems in social protection, including through the provision of benefits

relevant transformation could negatively affect a vast variety of fundamental rights as well as the relationship between citizens (or, more generally, welfare services' applicants) and public authorities. Digital welfare state's instruments, such as the nicknamed Robo-debt employed in Australia[16] or System Risk Indication (better known as SyRI) adopted by the Dutch Government with the purpose of detecting tax frauds and identifying illegitimate beneficiaries of public subsidies[17], as well as digital biometric identification systems proposed – and in some cases fully implemented – in several Global South

and other forms of assistance in various departments", DIGITAL FREEDOM FUND, *A litigation strategy on the digital welfare state. Towards a digital welfare state that centers on human needs*, August 2020, p. 1. Another definition can be found in Z. LARASATI – T.K. YUDA – A.R. SYFA'AT, *Digital welfare state and problem arising: an exploration and future research agenda*, in *International Journal of Sociology and Social Policy*, n. 1/2022: "In our definition, a digital welfare state (DWS) is a system of providing welfare services by the state based on the use of technology and data. (..) In our empirical observation, a DWS utilizes data that has been digitized by both the public and private sectors and is then processed by algorithms and artificial intelligence to produce effective and efficient policies concerning social services. Ultimately, the implementation of the DWS aims to ensure the target subjects of welfare service recipients and the social welfare redistribution efforts of the state are aligned", p. 2. What the authors interestingly and importantly underline is the three-steps transitional path towards a digital welfare state: in particular, "digitization begins with the conversion of analog data into digital data, which includes citizens' national identity data, education data, health data, employment data and others. In general, data collected by the government for the purpose of providing welfare services can be obtained from the sharing, purchasing and selling of data between the government and private sectors. After the data have been digitized, the next step is digitization. In the context of the recent trend toward a DWS, this step can be broadly defined as the widespread use of digital technology to support welfare decision-making processes and automate the process. In the digitization stage, a combination of technology and digitized data can be used to target welfare services to recipients based on their individual characteristics and needs, as in targeting health-care intervention. This idea supports the spirit of digital transformation, which aims to improve the quality of services and provide appropriate welfare services to citizens, especially marginalized groups, based on accessible data from the digital ecosystem. Having completed the digitization stage, the last step is digital welfare transformation, which describes changes in the process of providing welfare services", p. 5.

[16] The online compliance intervention (OCI) debt recovery system – colloquially named 'robo-debt' – has been adopted by the Australian Government with the main purpose of recovering social security 'overpayments'. Very briefly, this automated data processing instrument identifies errors or uncertainties in data and information provided by social services' beneficiaries; the system thus places the 'burden of proof' on the supposed debtors who are asked to 'disprove' the automated results produced by the robo-debt. On this criticized system, see P. SUTHERLAND, *Social security data-matching and Robodebts*, in *ANU College of Law. Legal Studies Research Paper Series*, n. 19/2018; T. CARNEY, *The new digital future for welfare: debts without legal proofs or moral authority?*, in *UNSW Law Journal Forum*, n. 1/2018; P. DUNLEAVY – M. EVANS, *Australian administrative elites and the challenges of digital-era change*, in *Journal of Chinese Governance*, n. 2/2019; T. CARNEY, *Robo-debt illegality: the seven veils of failed guarantees of the rule of law?*, in *Alternative Law Journal*, n. 1/2019; M. NIKIDEHAGHANI – J. ANDREW – C. CORTESE, *Algorithmic accountability: robodebt and the making of welfare cheats*, in *Accounting, Auditing & Accountability Journal*, August 2022.

[17] This system is based on an algorithm "designed to identify potential social welfare fraud (..). Following the linkage of many siloed datasets held by government agencies, the aggregated data were fed into the SyRI algorithm. The algorithm's risk model used several unknown risk indicators on the basis of which it detected increased risk of irregularities by generating risk profiles of cases suspected of presenting a higher likelihood of fraud. The submission of such a risk report could result in further investigation by relevant authorities", A. RACHOVITSA – N. JOHANN, *The human rights implications of the use of AI in the digital welfare state: lessons learned from the Dutch SyRI case*, in *Human Rights Law Review*, n. 22/2022, p. 2. The implementation of this instrument raised serious concerns which resulted, as we will better see later on in this paper, in "one of the first judgements in the world addressing the human rights implications of the use of AI in the public sector and states' respective obligations to ensure transparency of AI processes", decided by the District Court of first instance of The Hague, Decision *NCJM et al. and FNV v. The State of The Netherlands* C/09/550982 of 5 February 2020. On this controversial instrument, see S. RANCHORDAS, *Automation of public services and digital exclusion*, in *International Constitutional Law Blog*, 11th March 2020; M. VAN BEKKUM – F. ZUIDERVEEN BORGESIUS, *Digital welfare fraud detection and the Dutch SyRI Judgment*, in *European Journal of Social Security*, n. 4/2021.

Countries[18], have been at the center of a heated debate, sometimes involving Courts and having serious political consequences[19]. Based on massive collection, retention and control of a vast amount of personal data, these systems have been criticized by civil society representatives and NGOs and regarded as the first alarming step for the creation of an over-surveilled society impacting not only on privacy and data protection, but ultimately on non-discrimination and equality[20].

All these concerns have also drawn the attention of the UN Special Rapporteur on extreme poverty and human rights: in his 2019 Report, Philip Alston underlined that the "irresistible attraction" for Government to move towards a digital welfare state entails the "grave risk of stumbling, zombie-like, into a digital welfare dystopia"[21], often accompanied by budget restrictions, spending reviews and strong forms of conditionality[22].

Notwithstanding these relevant warnings, the threats caused by the welfare state's digitalization are still receiving little attention[23], especially if compared to the extensive political, judicial and ethical discussion that have accompanied the use of new technologies and Big Data for national and public security purposes after the 11th September 2001 terrorist attacks[24].

Considering this articulated and delicate context, the paper intends to shed light on the major challenges posed by the digital welfare state, the fundamental rights at stake as well as the role of different actors involved (legislators, civil society and courts), by focusing on a specific and relevant technological tool increasingly employed: the creation of national digital identities (IDs) through automated identification

[18] For a preliminary overview of the spread and use of automated identification systems, see MCKINSEY GLOBAL INSTITUTE, *Digital identification. A key to inclusive growth*, April 2019; PRIVACY INTERNATIONAL, *A guide to litigating identity systems*, September 2020.

[19] A clear example can be detected in the consequences of the abovementioned SyRI case in The Netherlands: after the abovementioned judgment (*supra* footnote n. 17) and a parliamentary report, both affirming the discriminatory nature and the lack of transparency of the automated system promoted by the Government, the Prime Minister Mark Rutte and his Cabinet resigned in January 2021, before the general elections scheduled for March.

[20] On this point, see the positions expressed by PRIVACY INTERNATIONAL, *A guide to litigating identity systems*, September 2020; CENTER FOR HUMAN RIGHTS AND GLOBAL JUSTICE OF THE NYU SCHOOL OF LAW, *Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID*, June 2022.

[21] P. ALSTON, *Report*, cit.

[22] A. MANTELERO, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Computer Law & Security Review*, n. 4/2018; V. GANTCHEV, *Data protection in the age of welfare conditionality: Respect for basic human rights or race to the bottom?*, in *European Journal of Social Security*, n. 1/2019.

[23] This trend seems to be confirmed by the limited number of papers documenting and exploring the challenges posed by the digitalization of welfare state as well as the judicial litigation concerning digital welfare instruments. In particular, as affirmed by Ranchordas, "the legal implications of digital inequality remain underestimated by lawyers and policymakers", S. RANCHORDAS, *Automation of public services and digital exclusion*, cit.; as it will emerge more in details in the next paragraphs, the implementation of digital tools employed in the welfare state sphere is not preceded, in most cases, by political debates and civil society's involvement or by surveys and preliminary studies assessing the risks for fundamental rights.

[24] The use of predictive policing as well as new sophisticated investigative instruments based on AI and Big Data – such as facial recognition technologies – have been at the center of a complex and wide discussion, involving legislators, courts, academics and civil society, especially after the Snowden's revelations: the literature as well as the case-law regarding the difficult balance between security and freedoms is vast and comprehensive.

systems, mainly relying on biometric data and employed as a mandatory condition to access vital welfare services.

In particular, after a brief analysis of the technical functioning and of the opportunities and critical aspects characterizing automated identification tools (para. 2), the adoption of these systems, representing a prominent and clear example of the issues posed by the welfare state digitalization process, will be explored in two specific Global South Countries: Jamaica and Kenya (para. 3). From a methodological perspective, this choice is motivated by the presence of significant similarities and common denominators that allow to determine common trends and solutions, consequently leading to shared considerations: both States are facing similar administrative and social problems, such as inequality, corruption, inefficiency of public authorities and welfare services, difficulty in correctly identifying citizens and guaranteeing a proper allocation of resources to the poorest categories of society – mostly living in rural areas. In both States a possible solution to these serious challenges has been determined in the proposed adoption of national identification systems able to create digital IDs using – also – a vast amount of biometric data; similarly, in both Countries the mandatory nature of these innovative identification tools and their exclusionary effects on already disadvantaged citizens, together with the lack of solid data protection and privacy laws, have raised serious concerns in civil society, NGOs and academics, leading to the intervention of national courts, asked to assess the lawfulness of the legislative framework adopted. In both these judicial litigations, Judges took long and complex judgments, carefully considering the proportionality and necessity of privacy-invasive instruments. As consequence, notwithstanding the different legal systems, traditions and Constitutional history, the approaches and solutions characterizing legislators' and courts' decisions in both selected Countries make a joint analysis possible and useful.

These thought-provoking case-studies ultimately result helpful for Western democracies, in which public authorities are more and more experimenting technological solutions based on the use of biometric data aiming at enhancing efficiency and cost savings in the welfare services' sphere[25].

The analysis developed in the central paragraphs will conclusively lead to some final remarks (para. 4) more generally concerning the role of different actors – courts, legislators and civil society – as well as the issues and possible solutions embedded in the gradual but profound shift towards a digital welfare state.

[25] The SyRI case, together with the controversial Irish Public Services Card, as we will see in the last paragraph, are perfect examples of the digitalization trend also characterizing Western Countries: the challenges and critiques these systems have drawn in recent years make it clear the need, also in the European context, to carefully evaluate the implementation of digital schemes and their effects on citizens. The considerations coming from different Countries that are similarly trying to adopt and promote a digitalization path of public assistance services can therefore reveal useful and valuable resources.

2. The Spread of National Biometric Digital IDs as Precondition for Accessing Welfare Services: 'Identification for Development' or 'Automating Inequalities'[26]?

The lack of proper legal and verifiable identity has been recognized as one of the main factors impacting on welfare states' efficiency and good governance: the absence of a unique identity causes the 'legal inexistence' of a person in front of State's authorities as well as the incapability of public welfare services to correctly allocate their limited resources to those in need[27]. Determining the identity[28] of citizens or social assistance's applicants is of crucial importance in order to avoid unlawful duplication of claims, prevent frauds, allow a more controlled access to benefits and facilitate a targeted allocation of public money or services to those meeting the eligibility criteria required.

The strict link between clear and recognized identities, the enjoyment of fundamental rights – especially the social ones –, the efficient functioning of welfare states and, consequently, the economic and social development has also been recognized at the international level: in fact, establishing legal identities for all has been identified as one of the UN Sustainable Development Goals – Target 16.9[29] – and has therefore become key objective of many international organizations. The World Bank Group, representing one of the largest sources of funding for developing countries, has vastly promoted and financed projects aimed at providing legal identities in many South Asian, Latin American and Sub-Saharan African Countries, by assisting governmental Institutions through the well-known ID4D (Identification for development) project[30]. According to the World Bank studies, identification represents a key enabler "of many other SDG goals and targets, such as financial and economic inclusion, social protection, healthcare and education, gender equality, child protection, agriculture, good governance, and

[26] These two expressions are borrowed, respectively, from the 'Identification for Development Initiative' promoted by the World Bank Group – see *infra* – and from the text written by V. EUBANKS, *Automating inequality: how high-tech tools profile, police and punish the poor*, New York, 2018.

[27] MCKINSEY GLOBAL INSTITUTE, *Digital identification*, cit.; C. SULLIVAN, *Digital identity: from emergent legal concept to new reality*, in *Computer Law & Security Review*, n. 4/2018; M.J. SULE *et al.*, *Cybersecurity through the lens of digital identity and data protection: issues and trends*, in *Technology in Society*, n. 67/2021.

[28] According to the UN Legal Identity Task Force, legal identity "is defined as the basic characteristics of an individual's identity, e.g. name, sex, place and date of birth, conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. (..) Proof of legal identity is defined as a credential, such as birth certificate, identity card or digital identity credential that is recognized as proof of legal identity under national law and in accordance with emerging international norms and principles", https://unstats.un.org/legal-identity-agenda/.

[29] Target 16.9: "By 2030, provide legal identity for all, including birth registration". The United Nations Legal Identity Agenda affirms that "everyone has the right to be recognized as a person before the law, as enshrined in Article 6 of the Universal Declaration on Human Rights and Article 16 of the International Covenant on Civil and Political Rights. (..) SDG Target 16.9 is key to advance the 2030 Agenda commitment to leave no one behind". On this target, see C. DUNNING – A. GELB – S. RAGHAVAN, *Birth registration, legal identity and the post-2015 Agenda*, in *CGD Policy Paper*, n. 46/2015.

[30] See the document WORLD BANK GROUP, *ID4D*, https://thedocs.worldbank.org/en/doc/325451527084344478019002201 8/original/ID4DProgramFlyerV52018.pdf.

safe and orderly migration"[31]. The Inter-American Development Bank too supported the creation of national IDs schemes, basing its support on the assumption that "not having a national identity document was found to have economic and financial implications and to be a determining factor in the cycle of poverty. To be undocumented means to be denied opportunities and possibilities to exercise civil and social rights"[32]. Moving from these considerations, providing trusted proof of identities to the almost 1 billion people in the world still lacking legal identity has been considered of paramount importance to, on the one hand, boost economic and social growth and unlock access to vital welfare services, especially to the most vulnerable, and, on the other hand, guarantee a correct management of public resources by properly identifying beneficiaries and minimizing frauds, biased decisions, waste of resources and malfunctioning.

Considering this scenario, the need to implement well-functioning and high-performance national identity systems has recently gained great momentum. In particular, digitalization and technological progress represent unprecedented resources able to help reaching the 'identification' goal, especially with reference to digital identities and automated biometric identity management schemes. Differently from traditional paper-based IDs, national digital IDs, meaning "a digitized representation of a person's legal identity"[33], can actually "be authenticated remotely, over digital channels"[34], thus allowing more efficient and reliable controls.

[31] See WORLD BANK GROUP, *Inclusive and trusted digital ID can unlock opportunities for the World's most vulnerable*, https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable. See also A. GELB – A. METZ, *Identification revolution. Can digital ID be harnessed for development?*, Washington D.C., 2018; A. BEDUSCHI, *Digital identity: contemporary challenges for data protection, privacy and non-discrimination rights*, in *Big Data & Society*, n. 1/2019.

[32] M.E. HARBITZ – M. TAMARAGO, *The significance of legal identity in situations of poverty and social exclusion: the link between gender, ethnicity, and legal identity*, Inter-American Development Bank Study, 2009.

[33] P. WALSHE, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, *Digital Identities*, T-PD(2020)04Rev, 26 October 2020.

[34] MCKINSEY GLOBAL INSTITUTE, *Digital Identification*, cit., p. 2.

In addition, the automation of identification systems[35] and the strengthening of their accountability through the use of biometric data have more and more taken hold[36]. Specifically, biometric identifiers are capable of attributing and correctly determining a person's identity: fingerprints, voice, facial photographs, hand geometry data, walking gait, DNA samples and iris scan fall under the category of biometric data, characterized by an irreplaceable and unique nature. By operating on the premise that physical biometric characteristics are distinctive and exclusive, biometric data has been rapidly used in identity management systems[37].

From a technical perspective, digital and automated biometric identification tools are built upon a complex process, starting with an enrollment phase during which a digital identity is created on the basis of personal and biometric data, collected and usually stored in centralized databases run by public agencies. Moreover, digital IDs schemes also establish a subsequent authentication phase, which opens every time a citizen or applicant needs to access public welfare services requiring the proper assessment of the ID: biometric and personal data collected at the moment of authentication are compared – through the use of algorithms and AI systems – to the entirety of data retained in the central repository; if there is a unique and positive match (so called one-to-many match), the identity is correctly verified and confirmed; otherwise, the consequences can be very severe: access to services is denied[38].

Considering all the potentialities and benefits in terms of accuracy and efficiency, here presented, the implementation of the described identification schemes, used as a mandatory requirement and a

[35] "Over the last 15-20 years, digital identity schemes have been increasingly framed as important means to fast and secure service provision. Digital identity schemes are schemes in which the three functions of identification, authentication and authorization are all performed digitally and hence differ from schemes in which, for example, the identity of users is ascertained through physical documents, but service delivery happens through digital means. (..) The link between digital identity scheme and socio-economic development is unpacked in multiple ways. Firstly, digital identity is seen as capable to provide secure recognition of public service users, making it possible to reduce exclusion errors from essential services. Digital identity is similarly viewed as a way to minimize the unlawful inclusion of non-entitled users in social welfare schemes, thus reducing inclusion errors. (..) The importance of digital identity platforms increases in the context of the identity deficit, meaning the gap between effective population and the number of people owning legal identity. Lack of a legal identity results in denial of rights", S. MASIERO – S. BAILUR, *Data-Driven Identities*, in S. SRIDHAR – A. PRAKASH – J. SRINIVASAN (eds), *Data-Centric Living: Algorithms, Digitisation and Regulation*, New York, 2022; see also S. BAILUR – S. MASIERO, *Digital identity for development: the quest for justice and a research agenda*, in *Information Technology for Development*, n. 1/2021 and in the same Journal A. MARTIN – L. TAYLOR, *Exclusion and inclusion identification: regulation, displacement and data justice*, n. 1/2021.

[36] MCKINSEY GLOBAL INSTITUTE, *Digital Identification*, cit., p. 2.

[37] J. WAYMAN – A. JAIN – D. MALTONI – D. MAIO (eds), *Biometric Systems*, Cham, 2005; E.J. KINDT, *Privacy and data protection issues of biometric applications*, New York, 2016; FRA (European Union Agency for Fundamental Rights), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, 2018; C. GRAZIANI, *La creazione di databases di dati biometrici: l'UE tra sfide alla sicurezza e data protection*, in L.E. RIOS VEGA – L. SCAFFARDI – I. SPIGNO (eds), *I diritti fondamentali nell'era della digital mass surveillance*, Naples, 2021.

[38] On this challenging aspect, see C. NYST – P. MAKIN – S. PANNIFER – E. WHITLEY, *Digital identity: issue analysis*, Guildford, 2016.

precondition to enable beneficiaries to access public vital welfare assistance and benefits, has increasingly become common in developing Countries[39].

But the growing interest in the adoption of such instruments, expressed by Governments all over the world, has been accompanied by strong oppositions: profound concerns have been expressed by academics, civil society and NGOs active in the field of fundamental rights protection. The storage of a vast amount of data – potentially covering the entire State's population – in a central database expose the retained information to significant threats, such as data breaches, un-authorized and unlawful access and function creep (namely the widening of the use of data beyond the identification purpose for which they were originally collected and retained, for example for security or investigative purposes). The presence of such a large amount of information could also facilitate profiling operations, using mathematical algorithms to combine and aggregate data coming from the authentication as well from the enrollment processes with other publicly available information in order to create a profile of citizens' habits, preferences, lifestyle, behaviors. This scaring scenario, far from being sci-fi, reveals how the potential intrusion in citizens' private sphere could be perpetrated by public authorities with the purpose of controlling, surveilling, investigating and even punishing[40]. In addition, the aformentioned dangers become even more complex and delicate when information collected and retained by the digital identification systems includes biometric data: the latter are not only unique and irreplaceable – once they are compromised or stolen, that cannot be reissued – but can also indirectly reveal other delicate and sensitive information, such as the presence or predisposition to certain diseases[41]. Furthermore, automated identification systems can't be considered unfailing in absolute terms, since also biometric data can, in some cases, modify over the time due to specific diseases (e.g. iris can change because of

[39] X. GINÉ *et al.*, *Use of Biometric Technology in Developing Countries*, in R. CULL – A. DEMIRGUC – J. MORDUCH (eds), *Banking the World: Empirical Foundations of Financial Inclusion*, Cambridge-Massachusetts, 2012; biometric identification systems are also increasingly employed by International Organizations in order to provide proofs of identity for refugees in emergency situations (the United Nations High Commissioner for Refugees has implemented a biometric systems to provide identity to Rohingya Muslim refugees in Myanmar in 2017, as reported by C. POPE, *Biometric data collection in an unprotected world: exploring the need for federal legislation protecting biometric data*, in *Journal of Law and Policy*, n. 2/2018); the spread of these systems in very delicate contexts, particularly involving fragile and vulnerable individuals, has been characterized – similarly to national digital IDs schemes – by critiques and concerns: on this point see A. FARRAJ, *Refugees and the biometric future: the impact of biometrics on refugees and asylum seekers*, in *Columbia Human Rights Law Review*, n. 42/2011; M. HU, *Biometric surveillance and big data governance*, in D. GRAY – S.E. HENDERSON (eds), *The Cambridge Handbook of Surveillance Law*, Cambridge-Massachusetts, 2017; OXFAM – THE ENGINE ROOM, *Biometrics in the humanitarian sector*, 2018; K. JACOBSEN – L. FAST, *Rethinking access: how humanitarian technology governance blurs control and care*, in *Disasters*, n. 2/2019; G. IAZZOLINO, *Infrastructure of compassionate repression: making sense of biometrics in Kakuma refugee camp*, in *Information Technology for Development,* n. 1/2021.

[40] G. VERMEULEN – E. LIEVENS (eds), *Data protection and privacy under pressure. Transatlantic tensions, EU surveillance and Big Data*, Bruxelles, 2017; A. KAUN, *Suing the algorithm: the mundanization of automated decision-making in public services through litigation*, in *Information, Communication & Society*, n. 0/2022.

[41] On this point, see the concerns expressed in the 2011 COUNCIL OF EUROPE Resolution 1797/2011, *The need for a global consideration of the human rights implications of biometrics* and by the UN HIGH COMMISSIONER FOR HUMAN RIGHTS in the Report *The right to privacy in the digital age*, August 2018.

diabetes, high blood pressure, glaucoma)[42]. Linking these systems and the automated identification procedure to the access to fundamental and vital services can potentially cause tragic effects, affecting to a greater extent the most vulnerable: a glitch or malfunctioning in the identification system could result in the denial of life-saving health services or food stamps for poor families and vulnerable people[43].

Then, it comes with no surprise that in some Countries, digital biometric identification tools used in the welfare sphere have been challenged before national Courts, amongst which the Jamaican and Kenyan ones.

3. The Crucial Role of Judicial Litigation: The Landmark Decisions of the Jamaican Supreme Court and the High Court of Kenya

In 2019 the Jamaican Supreme Court delivered an unprecedented and relevant ruling, halting the implementation of the so-called National Identification System (NIDS). Disciplined by the National Identification and Registration Act (NIRA) in December 2017, this instrument was aimed at creating a new digital ID for all Jamaican citizens and residents[44] and, very similarly to the Indian Aadhaar project[45],

[42] J. WAYMAN – A. JAIN – D. MALTONI – D. MAIO (eds), *Biometric Systems*, cit.; R. DUCATO, *I dati biometrici*, in V. CUFFARO – R. D'ORAZIO (eds), *I dati personali nel diritto europeo*, Turin, 2019.

[43] Automated systems and algorithms can't be considered infallible and unbiased: as confirmed by numerous studies, also AI schemes and programs can be biased or make mistakes due to malfunctioning or errors in the programming phase and in the data employed to "train" the artificial intelligence; on this controversial and highly debated aspect, see B. FRIEDMAN – H. NISSENBAUM, *Bias in computer systems*, in *ACM Transactions on Information Systems*, n. 3/1996; M. HILDEBRANDT, *Profiling and the rule of law*, in *Identity in the Information Society*, n. 1/2008; A. CHANDER, *The racist algorithm?*, in *Michigan Law Review*, n. 115/2017; O. OSOBA – W. WELSER, *An Intelligence in our image. The risk of bias and errors in AI*, Santa Monica, 2017; R.H. SLOAN – R. WARNER, *Beyond bias: AI and social justice*, in *Virginia Journal of Law & Technology*, n. 1/2020; S. TOMMASI, *Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo*, in *Revista de Direito Brasileira*, n. 10/2020; K.M. KOSTICK-QUENET *et al.*, *Mitigating racial bias in machine learning*, in *The Journal of Law, Medicine & Ethics*, n. 1/2022.

[44] According to Section 2 of the NIRA, also residents for more than six months are required to enroll to the national IDs scheme.

[45] The Indian Aadhaar project, based on the collection and retention in a centralized repository of biometric data (fingerprints, photos, iris scan), is the biggest biometric identification system in the world. After the enrollment procedure, residents are given a unique 12-digit number which represents a mandatory and compulsory requirement in order to access public welfare services, such as government benefits, pensions, food stamps and subsidies. The system was increasingly extended to other public services such as school enrollment, driving license and was also gradually demanded by private entities (e.g. digital identity was considered necessary to open a bank account or to obtain a telephone number). Through the creation of such a gigantic identification system, the Indian Government aimed at preventing money laundering, resource waste and frauds, detecting identity theft and guaranteeing a targeted allocation of benefits, ensuring that they can reach the intended beneficiaries. While the system was first introduced and developed in 2009, a specific legislative framework (the Aadhaar Bill) was approved by the Indian Parliament only in 2016: the unclear and opaque legal basis, the limited safeguards and the lack of an overall federal legislation guaranteeing privacy and data protection, together with data security vulnerabilities (some data breaches and data leaks were also confirmed by public authorities) were at the center of a great number of petitions; applicants were also worried about the program's impact on the most vulnerable and rural communities, where malfunctioning and denial of services' access could lead to severe consequences. The central database, retaining unique biometric data, has been considered able to expose citizens' very sensitive information to data breaches or profiling operations perpetrated by public authorities: law enforcement authorities, for example, were authorized to access the repository for purposes different from the identification one, among which national security reasons, without precise limitations or specific determination of

it was based on the collection and retention in a central repository of a vast amount of demographic[46] and biometric data: facial image, fingerprint, eye color, manual signature, together with other data that could be eventually added (specifically retina or iris scan, vein pattern, footprint and blood type). The new compulsory digital ID was considered by the Jamaican Government a viable and efficient solution to both fight against endemic challenges concerning public authorities (e.g. corruption, inefficiency, frauds, waste of public resources) and provide the population with a clear and unique identity; for these reasons the NIDS was promoted, also thanks to important loans provided by the Interamerican Development Bank, as unique automated verifier of Jamaicans' identities, able to substitute other existing different IDs (f.i. tax registration number, electoral IDs, passport).

Notwithstanding these potentialities, NIRA was, since the beginning, firmly criticized by civil society as well as by Parliamentary Opposition, denouncing the possible negative impacts of such scheme on fundamental rights' protection. These fears were first of all founded on the lack of specific provisions regulating the processing and retention of sensitive data collected, mainly aggravated by the absence of a solid legal framework ensuring privacy and data protection[47] at the time NIRA was approved; furthermore, the provisions allowing, in vast terms, law enforcement authorities to access the central database for the general interest of fighting and preventing crime and corruption[48], raised additional concerns on the risks of function creep and possible abuses and misuses of data initially collected for identification purposes only. The compulsory nature of the digital ID, reinforced by criminal sanctions and convictions[49] inflicted upon those who didn't enroll, was considered by the Act's opponents able to produce serious exclusionary effects, mainly affecting the most vulnerable segments of the population,

possible uses. Moreover, also the 'authentication data' (revealing the reason why the citizen needs his/her identity to be assessed, the service he/she needs to access and where the authentication is required) were collected and retained: according to the applicants, this unproportioned gathering of information could ultimately drive to a 'mass surveillance society' where all citizens are controlled and profiled by public authorities. All these critical aspects were ultimately considered by the Supreme Court in the well-known case *Justice Puttaswamy v. Union of India*, 26th September 2018 (D.N. 35071/2012). For an in-depth analysis of this system as well as of its criticalities and negative effects, see P. DIXON, *A failure to "Do no harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*, in *Health and Technologies*, n. 6/2017; S. MASIERO, *Explaining trust in large biometric infrastructures: a critical realist case study of India's Aadhaar project,* in *Electronic Journal of Information Systems in Developing Countries*, n. 6/2018; R. KHERA (ed), *Dissent on Aadhaar: big data meets big brother*, New Delhi, 2019; N. ANAND, *New principles for governing Aadhaar: improving access and inclusion, privacy, security and identity management*, in *Journal of Science Policy & Governance*, n. 1/2021.

[46] Information on religion and racial origins were optional.

[47] The Data Protection Act only passed in June 2020, after a long legislative debate. On this Act, see G. GREENLEAF, *Jamaica adopts a post-GDPR data privacy law*, in *Privacy Laws & Business International Report*, n. 1/2020.

[48] According to Section 45, requesting entities can ask the authority managing the digital IDs system to authenticate the applicant's identity; by using the data contained in the database, the authority was not allowed to disclose core biometric information. In certain cases, the Court could grant an order to disclose biometric and demographic information retained in the database for prevention or detection of a crime, national security, public emergency and investigations.

[49] Section 20, para. 11, NIRA.

such as citizens who lacked birth certificates necessary to access the registration procedure and people who couldn't afford to request them.

These oppositions and doubts were partly confirmed in 2019 by the Supreme Court in the famous ruling *Julian J. Robinson v. The Attorney General of Jamaica*[50]: in that case, the Judges ended up declaring the NIRA unconstitutional, null, void and of no effect, also providing important guidance to the national legislator on the proportionality and necessity of a national digital ID scheme in a democratic society.

Interestingly and vastly quoting the Indian Justice Chandrachud's dissenting opinion in the Aadhaar case[51], the Jamaican Supreme Court recalled the twofold nature of the constitutionality test: to firstly determine if fundamental rights are impacted and then to establish whether the measure limiting constitutional rights is justified in a free and democratic society, namely if "i) the objective of the offending statute is of sufficient import to warrant the override of the right; ii) the means by which the objective is to be achieved is proportional, meaning the measures must be carefully designed to achieve the objective. They cannot be arbitrary, unfair or irrational; iii) the measures should impair as little as possible the right in question; iv) the effect of the measure must be proportionate to the sufficiently important objective. The more severe the effect of a measure the more important must be the objective",

[50] Claim no. 2018HCV01788, 12 April 2019. It is important to underline that Section 19 (1) of the Jamaican Constitution permits any person to apply to the Supreme Court for constitutional remedies if "any of the provisions of this Chapter [of the Charter] has been, is being or is likely to be contravened in relation to him". On Jamaican Constitution see S. VASCIANNIE, *The Constitution and the rule of law: some recent developments in Jamaica*, in *Commonwealth Law Bulletin*, n. 1/2009; R. ALBERT – D. O'BRIEN – S. WHEATLE (eds), *The Oxford handbook of Caribbean Constitutions*, Oxford, 2020.

[51] In the abovementioned (footnote n. 44) ruling of the Indian Supreme Court on the national biometric IDs scheme, the Judges considered the system in its entirety proportionate and legitimate, whereas only some specific parts – the most relevant being the mandatory requirement of the Aadhaar number by private entities or the vague and arbitrary access to biometric data by law enforcement authorities – were considered unlawful. Although the majority assessed that the "the Aadhaar has struck a fair balance between the right to privacy of the individual with the right to life of the same individual as beneficiary" of subsidies and welfare services, recognizing the Aadhaar systems as a "vital tool for ensuring good governance in a social welfare state", Justice Chandrachud addressed what has been defined a "dissent for the age" (G. BATHIA, *The Aadhaar judgment: a dissent for the age*, in *Indian Constitutional Law and Philosophy*, 27th September 2018). Starting by affirming that "denial of subsidies and benefits to Indian citizens due to the infirmities of biometric technology is a threat to good governance and social parity", the dissenting Judge considered the identification system too invasive with respect to privacy and data protection, not passing the proportionality test and not respecting data minimization principles: the system "severely impairs informational self-determination, individual privacy, dignity and autonomy". Praised by Indian NGOs' activists and civil society, this dissenting opinion was largely quoted by the Jamaican Supreme Court, thus representing a perfect example of how dissent can find fertile soil in different Countries, other than home. It comes with no surprise that the Jamaican decision on the legitimacy of NIRA has been named "the afterlife of the Aadhaar dissent" (G. BATHIA, *The afterlife of the Aadhaar dissent: the Jamaican Supreme Court strikes down a national biometric identification system*, in *MediaNama*, 15th April 2019); on the abovementioned dissenting opinion, see also R. KRISHNA, *Data management in India: a case study of Aadhaar Project*, in S. KUMARI – K.K. TRIPATHY – V. KUMBHAR (eds), *Application of Big Data and business analytics*, Bingley, 2020; A. PADMANABHAN – V. SINGH, *The Aadhaar verdict and the surveillance challenge*, in *Indian Journal of Law and Technology*, n. 1/2019; V. BHANDARI – R. SANE, *Critique of the Aadhaar legal framework*, in *National Law School of India Review*, n. 1/2019; G. FORMICI, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti*, in *DPCE Online*, n. 2/2019; A. DHINDSA, *Hope in dissent*, in *Supremo Amicus*, n. 10/2019; S. CHHUGANI, *India's Aadhaar card: a violation of Indian citizen's right to privacy*, in *Cardozo International & Comparative Law Review*, n. 2/2021; JAMILA, *Supreme Court's verdict on privacy. Analysis of the Puttaswamy case*, in *Jus Corpus Law Journal*, n. 3/2021.

para. 343. Applying this test in a 309 pages-long decision, the Court clearly affirmed, in a crucial sentence worth being entirely reported, that "the mandatory nature of the requirement as well as the breadth of its scope, and the absence of a right to opt out, are not justified or justifiable in a free and democratic society. If it is intended to prevent corruption or fraud, then it is premised on the assumption that all Jamaicans are involved with corruption and fraud. The danger of abuse by the state or its agencies and the removal of personal choice, outweigh any conceivable benefit to be had by the community or state", para. 349.

In particular, according to the Court, large-scale collection, retention and proceeding of data, some of which irreplaceable by nature, translates "into a great power over the lives of persons" (para. 237) and represents an extensive invasion into the private sphere[52] and the 'informational privacy'[53]: "the very real prospect of control by data, and of big brother tracking your every move, is the antithesis of freedom in a democratic state", para. 355. This limitation of constitutional rights and the risks deriving from authentication provisions – allowing public authorities to verify applicants identities by using priorly collected and retained information –, didn't result to be properly balanced by solid and comprehensive safeguards; in fact, the Court highlighted how NIRA "fails to prohibit sharing of such information at the time of verification or authentication, or to require the individual's consent. It has no time limit on the retention of such information"[54].

Ultimately, the coercing nature of the identification scheme – together with the imposition of a criminal offence punishing the failure to enroll – was found disproportionate to any benefit: by preventing people from accessing vital public services, the mandatory enrollment was considered able to impact not only

[52] The Charter of Fundamental Rights and Freedoms, adopted through the Charter of Fundamental Rights and Freedoms (Constitutional Amendment) Act of 2011, repealed Chapter 3 of the 1962 Constitution. The actual Constitution thus recognizes, amongst the others, the right "of everyone to i) protection from search of the person and property; ii) respect for and protection of private and family life, and privacy of home; iii) protection of privacy of other property and of communication" (Chapter 3, Section 13, 3, lett. j), as well as the "right to equitable and human treatment by any public authority" (Chapter 3, Section 13, 3, lett. h). On the Charter of Fundamental Rights and Freedoms, see D. O'BRIEN – S. WHEATLE, *Post-independence Constitutional reform in the Commonwealth Caribbean and the new Charter of Fundamental Rights and Freedoms for Jamaica*, in *Public Law*, n. 4/2012; S. WHEATLE, *The rights to equality and non-discrimination and the Jamaican Charter of Fundamental Rights and Freedoms*, in *West Indian Law Journal*, n. 126/2012.

[53] Meaning the control over personal information. For an in-depth analysis of the examined decisions, see H. S. DUNN, *Risking identity: a case study of Jamaica's short-lived national ID system*, in *Journal of Information, Communication and Ethics in Society*, n. 3/2020.

[54] Para. 360. The vast terms used to allow disclosure of identity information have been considered incompliant with the Jamaican Constitution and more stringent controls and adequate protections have been declared necessary to prevent possible abuses. As Justice Sykes CJ underlined, no independent oversight body is mandated to conduct an audit and to verify the respect of NIRA by public authorities (para. 249): "compulsory taking of biographical and biometric data is a violation of privacy rights (..). There is no evidence that the data required under the Third Schedule [of the NIRA] is the minimum necessary to identify persons and so there is no evidence that the right to privacy has been violated as little as possible. There is no evidence that the concept of data minimization, which is taking no more than is necessary to meet the objective was applied in the drafting of the Third Schedule" (para. 250). Data minimization and necessity test were identified as fundamental criteria to evaluate the legitimacy of biometric and digital IDs systems.

the right to life, liberty and security of the persona[55] but also the right to equality before the law[56]. The Court was very clear on this point: "there is no doubt that if one chooses to access public services it is normally necessary to satisfy that entity of one's identity. That is not what makes Section 41 [NIRA] offensive. Section 41 is unconstitutional because it purports to make a national identification card or number the only method of verification of identity", para. 363.

In conclusion, by considering the unconstitutionality of the abovementioned key provisions of the NIRA as able to nullify the act in its entirety, Justice Sykes additionally provided significant and useful evaluations for possible future developments: "the regime as it presently stands does not offer sufficient protection for the sensitive data that is to be collected under the statute. This means that even if the scheme were a voluntary one, more robust protection would be required" (para. 261); in other words, the presence of a proper legal framework, establishing precise guarantees and safeguards, was deemed of paramount importance to legitimately implement privacy-invasive instruments. Moreover, although the possibility to adopt digital IDs schemes and biometric management systems was not *per se* denied, the Court recognized the possible negative impacts on fundamental rights as well as the potential exclusionary effects; based on these considerations, minimization of data required, opt-out possibilities, strong safeguards against abuses, independent authorities' oversight and the creation of inclusive policies able to limit discriminatory results emerged as necessary requirements.

After this landmark decision, in September 2020 the Jamaican Government announced a new legislative initiative aimed at establishing a reformed National Identification System able to properly consider the criteria and requirements established by the Court. This process finally led to a renewed National Identification and Registration Act, approved in 2021[57]: Prime Minister strongly reaffirmed not only the importance of a digital IDs scheme, defined as a step towards the achievement of the 2030 UN SDGs – in particular social protection and effective governance –, but also the correctness and appropriateness of the comprehensive revisions introduced, able to properly take into account the Court's ruling and the principles enshrined. Specifically, the reformed identification scheme is now voluntary and criminal offences linked to the absence of a digital ID have not been reconfirmed. The biometric information required to enroll has been sensitively restricted, now including facial image, fingerprints and manual signature; the possibility for law enforcement authorities to access the central database where collected sensitive data are stored is permitted for investigation, prevention and detection of crime or interest of

[55] Chapter 3, Section 13, 3, lett. a), Jamaican Constitution.
[56] Chapter 3, Section 13, 3, lett. g), Jamaican Constitution.
[57] This new NIRA followed a long legislative path, started in December 2020, when the new draft bill was proposed; the Government also promoted the creation of a Joint Select Committee formed to review the new Bill. Organisations and individuals were allowed to participate to the public debate by making submissions to the Committee. To learn more on the current legislation, see https://www.nidsfacts.com.

national security; a National Identification and Registration Inspectorate will also be established in order to ensure the compliance and respect of the Act and the correct managing and functioning of the system itself.

Although the new NIDS will be presumably fully operational by the end of 2022[58] and notwithstanding the relevant revisions introduced, the new Bill has not quieted concerns and critiques. In particular, NGOs and civil society underlined persistent problems and criticalities affecting the revised system: the possible negative exclusionary effects of the approved identification scheme have not been properly addressed by the legislator, who failed to consider the real and concrete difficulties poor and vulnerable segments of the population could face due to the lack of birth certificates or other documents required for the enrolment procedure[59]; more importantly, if it is true that the Data Protection Act passed in June 2020[60], marking a paramount evolution and strengthening towards a solid data protection in Jamaica, the Act doesn't result to be not fully in force at the moment, due to a 2-years implementation period – ending in late 2023 – granted to data controllers; this seems to translate in a persistent lack of those comprehensive safeguards strongly required by the Supreme Court[61].

The relevant and profound modifications introduced by the most recent NIRA undoubtedly show a positive trend: facing the strong determination of the Jamaican Government to implement a national digital IDs scheme, the Court's intervention urged policymakers and legislators to attentively evaluate the impact of pervasive collection and processing of personal data on fundamental rights. Nonetheless, the absence of well-functioning and comprehensive data protection provisions as well as the concrete difficulties part of the Jamaican population could face during the enrolment procedure, still cast a shadow on the future developments of the Jamaican NIDS.

---

[58] According to the expected timeline established by the Government and available at https://www.nidsfacts.com. Some pilot programs are planned to be undertaken in Kingston and St Andrew, with the purpose to anticipate the full-scale national enrolment phase.

[59] According to the Government announcements, the "Project Birthright" initiative will be launched in order to "supply the important document to eligible Jamaicans who fall below a certain income threshold" (see the News "Over 11000 Jamaicans to receive birth certificates under 'Project Birthright", 31st May 2022, https://www.nidsfacts.com/over-11000-jamaicans-to-receive-birth-certificates-under-project-birthright/).

[60] See footnote n. 47.

[61] On this point, see the considerations and concerns expressed by 13 Organizations and NGOs in the *Submission to the Joint Select Committee of Parliament reviewing the NIRA*, February 2021, https://nidsfocus.com/wp-content/uploads/2021/04/NIDS-Coalition-Submission-Feb-2021.pdf. Jamaicans for Justice and other civil society organizations warned about possible risks, among which they listed: "Significant components of the legal framework for NIDS have been left to future regulations; interpretation of this Bill is incomplete without the Data Protection Act's regulations in place; NIDS should not be made *de facto* mandatory; collecting biometrics endangers the individual and the system"; as a consequence, the stakeholders recommended various modifications to the proposed bill: in particular, to minimize the data necessary for enrolment, to collect additional information only optionally; to make the Data Protection Act fully operational prior to bringing the NIDS into force; to strengthen parameters and safeguards for disclosures of information to third parties; to affirm a right to know about disclosures of personal information as well as the right to erasure of information; to minimize the risks of disclosure for authentication records/logs and to support vulnerable persons in all service interactions.

Similarly to what happened in Jamaica, the Kenyan National Integrated Identity Management System (NIIMS), popularly known with the Swahili term 'Huduma Namba', has been – and remains – at the center of a complex debate.

In 2018, the Kenyan Parliament approved the Miscellaneous Amendments Act[62] introducing, amongst the other modifications, also a digital identity scheme for all citizens and residents[63]. The national digital ID and the associated identification management system were intended to create a mandatory and unique source of personal identification and were based on the collection, retention and proceeding of a vast range of data, encompassing not only biometric data such as fingerprints, iris scan, hand geometry and voice waves but also, and more surprisingly, DNA and GPS coordinates of the place of residence.

After a mass biometric registration initiative in March 2019, aimed at collecting the biometric data necessary for the enrollment phase and the subsequent issuing of the identification number and card, several NGOs and civil society representatives raised profound concerns about the lack of transparency affecting both the approval procedure of the scheme and its functioning, the absence of a proper national legal framework on privacy and data protection ensuring important safeguards to data collected as well as the concrete risk of exclusion from vital benefits to the detriment of marginalized groups in rural areas. Based on these considerations, which present profound similarities with those expressed in the Jamaican case here examined, the Nubian Rights Forum, the Kenya Human Rights Commission and the Kenya National Commission on Human Rights – supported by other NGOs and civil society associations – filed several petitions to the High Court, claiming that the approved Huduma Namba "pose serious and immediate threats to fundamental rights and freedoms protected under the Bill of Rights"[64].

In its long awaited and crucial decision *Nubian Rights Forum and Others v. The Hon. Attorney General*, published the 30th January 2020[65], the High Court in Nairobi didn't deny the legitimacy of the NIIMS *per*

[62] Miscellaneous Amendments Act No. 18, January 2019.

[63] See Section 9A, 2a).

[64] Para. 5, High Court ruling on Petitions 56,58,59 of 2019, *Nubian Rights Forum et al v. The Cabinet Secretary, Ministry of Interior et al.*, 30th January 2020. It appears useful to underline that the The Bill of Rights was introduced in 2010 Constitution: M.K. MBONDENYI – J.O. AMBANI, *The new constitutional law of Kenya: Principles, Government and Human Rights*, Nairobi, 2012; M.K. MBONDENYI – S.O. ODERO – P. LUMUMBA, *The Constitution of Kenya*, Nairobi, 2013; K. R. HOPE, *Bringing in the future in Kenya: beyond the 2010 Constitution*, in *Insight on Africa*, n. 2/2015; M. KENSON, *The Constitutional context of human rights defenders in Kenya under the 2010 Constitution*, 2020, available at SSRN: https://ssrn.com/abstract=3725831.

[65] This decision was preceded by an interim order adopted by the High Court of Nairobi in April 2019 (Consolidated Petitions no. 56, 58, 59 of 2019, *Nubian Rights Forum et al. v. The Attorney-General*): through this intervention, the Judges restricted the Government to fully implement the NIIMS until the case conclusion, by also impacting on the already started Huduma Namba enrollment phase. In particular, the Government was precluded from making national biometric ID scheme registration mandatory, from collecting DNA or GPS, from setting any deadline for registration and from sharing the collected data with third parties. On this point see M. NYAWA, *The Big Brother is watching: Huduma Namba a threat to our rights and freedoms*, 2019, available at http://dx.doi.org/10.2139/ssrn.3389268; M. ODDEN, *Biometric crisis: legal challenges to biometric identification initiatives*, in *Wisconsin International Law Journal*, n. 2/2022; G. MUTUNG'U, *The*

se: despite recognizing the severe risks posed by massive collection and retention of personal and biometric data as well as the possible exclusionary effects of a mandatory digital identification system, the Judges halted the implementation of the IDs scheme only until a comprehensive regulatory framework, able to address all the side effects and criticalities emerged in the decision, is adopted. The only provisions entirely considered unconstitutional[66] – specifically in violation of Art. 31 of the Kenyan Constitution[67] – have been identified in the inclusion of genetic and location data amongst the information necessary to obtain a digital ID. In particular, on this relevant point, the Court affirmed that "unlike other biometric characteristics, the technique used in DNA identification, which is a DNA comparison process, does not allow for the verification or identification to be done in real time, the comparison is also complex, requires expertise and takes time. (..) Lastly, we also find that the necessity of GPS monitors in identification is even less evident", para. 780-781.

Differently from the collection and processing of location and genetic data, regarded as unnecessary and unjustified, the use of biometric data was considered necessary for the purpose of identification: "other than the DNA and GPS coordinates, information to be collected pursuant to the impugned amendments to the Registration of Persons Act is necessary and is therefore not unconstitutional", para. 777. But the legitimization, in general terms, of biometric IDs schemes didn't come without limitations or conditions; in fact, the Judges proceeded in their exam of the impugned legislation by recognizing, first of all, the potential risks and severe dangers linked to the absence of a clear legal framework: "the misuse [of the collected biometric data] can result in discrimination, profiling, surveillance of the data subjects and identity theft. In addition, as a result of the central storage of biometric data, in most cases the data subjects have no information or control over the use of his or her biometric data", para. 880. In order to be regarded as proportionate and necessary, "all biometric systems (..) require a strong security policy and detailed procedures on its protection and security which comply with international standards", para. 883. And it is exactly by looking at these specific requirements that the Court found serious criticalities: "although a legal framework for protection of personal data now exist in Kenya, there are inadequacies

UN guiding principles on business and human rights, women and digital ID in Kenya: a decolonial perspective, in *Business and Human Rights Journal*, n. 1/2022.

[66] As affirmed in para. 541 of the analysed ruling, Art. 165, para. 3, lett. d, ii) of the Kenyan Constitution establishes that the High Court shall have jurisdiction to hear any question respecting the interpretation of the Constitution, including the determination "of the question whether anything said to be done under the authority of this Constitution or of any law is inconsistent with, or in contravention of, this Constitution".

[67] "Every person has the right to privacy, which includes the right not to have (a) their person, home or property searched, (b) their possessions seized; (c) information relating to their family or private affairs unnecessarily required or revealed; or d) the privacy of their communications infringed". Information privacy is included in this definition, meaning "the rights of control a person has over personal information". See also the decision *Kenya Legal and Ethnic Network on HIV & AIDS et al. v. Cabinet secretary Ministry of Health et al.* which affirmed and clarified the content of the right to privacy in Kenya.

in the said legal framework in terms of operationalization and also in terms of the implementation and operationalization of NIIMS, to guarantee the security of the data that will be collected in NIIMS", para. 911. In other words, although biometric data, differently from other information such as genetic data or GPS coordinates, are necessary for identification procedures and can thus be collected and processed, "an inadequate legislative framework for the protection and security of the data is" not only "a clear limitation to the right to privacy, in the light of the risks it invites for unauthorized access and other data breaches" (para. 920) but also "contrary to the principles of democratic governance and the rule of law" (para. 922). The guarantees included in the Act adopting the NIIMS as well as in the Data Protection Act – which came into force in November 2019, after the Petitions were filed[68] – were not considered sufficient and adequate to limit the intrusion into the private sphere and the risks of function creep and surveillance. Evaluating the national discipline on data protection, the Court interestingly noted that a regulatory framework needs to be properly enforced in order to be effective: "the implementation of the Data Protection Act 24 of 2019 requires an implementation framework to be in place, including the appointment of the Data Commissioner, as well as the enactment of operational regulations", para. 853. Therefore, after recognizing the persistent absence of a robust set of rules and safeguards on data proceedings, the Judges exposed a significant consideration, that will be more vastly underlined later on in the conclusive remarks: "the process of NIIMS appeared to have been rushed" (para. 922), not being anticipated by a specific, clear, comprehensive and unambiguous legislation[69].

[68] Data Protection Act, no. 24 of November 2019. On data protection in Kenya, see A.B. MAKULILO – P. BOSHE, *Data protection in Kenya*, in A.B. MAKULILO (ed), *African data privacy laws*, in *Law, governance and technology series*, n. 33/2016 – providing an analysis of the data protection in Kenya before the 2019 Act –; R. ALUNGE, *Consolidating the right to data protection in the information age: a comparative appraisal of the adoption of the OECD (revised) guidelines into the EU GDPR, the Ghanaian Data Protection Act 2012 and the Kenyan Data Protection Act 2019*, in J. THORN – A. GUEYE – A. HEJNOWICZ (eds), *Innovations and interdisciplinary solutions for underserved areas. InterSol 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Cham, 2020; N. JACKTONE, *the data protection vis a vis the developments around e-commerce in Kenya*, 2020, available at http://dx.doi.org/10.2139/ssrn.3840; F. MBOGORI, *Legal challenges facing algorithmic decision-making in Kenya*, 2021, available at http://dx.doi.org/10.2139/ssrn.3940381; B. DAIGLE, *Data Protection Laws in Africa: Pan-African survey and noted trends*, in *Journal of International Commerce & Economics*, n. 1/2021; H. MUKIRI-SMITH – R. LEENES, *Beyond the 'Brussels effect'? Kenya's Data Protection Act (DPA) 2019 and the EU's General Data Protection Regulation (GDPR) 2018*, in *European Data Protection Law Review*, n. 4/2021; P. BOSHE – M. HENNEMANN – R. VON MEDING, *African Data Protection Laws: current regulatory approaches, policy initiatives, and the way forward*, in *Global Privacy Law Review*, n. 2/2022.

[69] These considerations have been reaffirmed by the Court in another subsequent ruling on Huduma Namba: while the examined *Nubian Rights Forum* case was pending, the Government announced, through a press statement published on 18th November 2020, the rollout of the Huduma Card, issued on the basis of biometric data obtained during the first mass collection of data in March 2019. This statement immediately appeared to be in contrast with the interim order previously pronounced by the High Court (see footnote n. 65) and was consequently opposed by several NGOs which filed a judicial review application for orders of certiorari, mandamus and prohibition of the rollout procedures. On 14th October 2021, the Court declared the implementation of the Huduma Namba Card illegal due to the lack of the proper data protection impact assessment specifically required by Section 31 of the Data Protection Act; this law was already effective when the analyzed petition was submitted but was not operative at the time the first mass collection of biometric data – necessary to the rollout of the Huduma Card – was implemented in 2019. In the decision *Republic of Kenya v. Joe Mucheru, Cabinet Secretary Minister of Information Communication and Technology et al. & Katiba Institute, Yash Pal*

Another very delicate criticality tackled in the ruling concerns the petitioners' claims on the discriminatory nature of the proposed biometric ID system: the Judges clearly underlined the importance of establishing legislative solutions able to find a proper balance-point between efficiency objectives, pursued by the identification scheme, and the serious consequences this kind of tools could cause on the most disadvantaged segments of the population. Following this reasoning, the Court expressed the necessity to adopt adequate safeguards and alternative non-digital instruments intended to ensure access to fundamental welfare services in case technical malfunctioning or lacking documentation occur. In particular, birth certificates or national identity cards, indicated as prerequisites to activate the NIIMS enrollment procedure, could represent a significant barrier and obstacle for vulnerable and poor communities, mostly living in rural areas, in a Country where only 67% of births are registered[70]. Even if the highlighted concrete risks of exclusion have not been considered sufficient to declare a violation of the right to non-discrimination recognized at Art. 27 of the Kenyan Constitution[71], the Court clearly affirmed: "in our view, there may be a segment of the population who run the risk of exclusion for the reasons already identified in the judgement. There is thus a need for a clear regulatory framework that addresses the possibility of exclusion in NIIMS. Such a framework will need to regulate the manner in which those without access to identity documents or with poor biometrics will be enrolled in NIIMS. Suffice to say that while we recognize the possibility of this exclusion, we find that it is in itself not a sufficient reason to find NIIMS unconstitutional" with regard to non-discrimination (para. 1012).

In conclusion, this long ruling – vastly recalling the Aadhaar case but also international or European documents (such as the Reports of the UN High Commissioner for human rights on the right to privacy or the EU Agency for Fundamental Rights' report on the fundamental rights implications of storing

Ghai and Data Commissioner, KEHC 122 (KLR), the High Court affirmed the retrospective effect of the Data Protection Act: "the need to protect the constitutional right to privacy did not arise with the enactment of the Data Protection Act; the right occurred from the moment the constitution was promulgated", with particular reference to Art. 31 of the Constitution; accordingly, "it would have been prudent (..) for the State to ensure that the legal framework for protection of the right to privacy was in place before taking action likely to infringe the individual's right under Art. 31 of the Constitution. Considering the object and purpose of the Data Protection Act, and more importantly, considering that the Act was intended to give effect to Art. 31, c) and d) of the Constitution, it would have been reasonable to have the Act in place before the purported amendment [establishing the rollout] (..) and before the collection and processing of personal data" (para. 13). Following these evaluations, the Court accused – once again – the State of choosing "to put the cart before the horse" (para. 104).

[70] According to the data provided by the World Bank and available at https://data.worldbank.org/indicator/SP.REG.BRTH.ZS?end=2014&locations=KE&start=2003&view=chart. See also M. FREYTSIS *et al.*, *Development of a mobile self-sovereign identity approach for facility birth registration in Kenya*, in *Frontiers in Blockchain*, 15th February 2021.

[71] "Every person is equal before the law and has the right to equal protection and equal benefit of the law. Equality includes the full and equal enjoyment of all rights and fundamental freedoms (..). The State shall not discriminate directly or indirectly against any person on any ground, including race, sex, pregnancy, marital status, health status, ethnic or social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth", Art. 27, Kenyan Constitution.

biometric data in identity documents and residence, dated 2018), GDPR provisions, Reports of Art. 29 Data protection working party of the EU and landmark case-law of the ECtHR, but also of USA, Canadian, Indian and African Courts – limited on the one side the possibility for the Kenyan Government and Parliament to establish an identification system based on the collection and processing of DNA and GPS coordinates, but on the other side confirmed that "The respondents are at liberty to proceed with the implementation of the NIIMS and to process and utilize the data collected in NIIMS only on condition that an appropriate and comprehensive regulatory framework on the implementation of NIIMS that is compliant with the applicable constitutional requirements identified in this judgement is first enacted", para. 1047. This position, while warning on possible risks for different fundamental rights, opened the doors to a renewed political and legislative debate.

In fact, similarly to what happened in Jamaica, in 2021 a reformed Huduma Namba Bill[72] was submitted with the purpose of establishing a new primary law on legal identification management, regulating the NIIMS as well as the connected database. This proposal is still under discussion before the Kenyan Parliament[73] and its future developments will surely be affected by the – still controversial – results of August general elections[74]. Notwithstanding its uncertain path[75], the proposed identification scheme has drawn once again the attention of civil society organizations and NGOs, who have already manifested their concerns[76]: according to several stakeholders, indeed, the draft bill does not efficiently answer to the criticalities and deficiencies underlined by the High Court in the above analyzed decision; in particular, the possible side effects in terms of exclusion and discrimination were not properly considered and the risks for people who do not possess identification documents or birth certificates (also including street families, street children and stateless persons) or have biometric challenges, remain mainly unaddressed.

[72] National Assembly Bill no. 57 of 2021.

[73] This Bill is still under discussion before the Parliament: the scheduled 13th July 2022 debate session (third reading), aimed at discussing the proposed amendments to the Bill, has been postponed.

[74] After 9th August 2022 elections, William Ruto has been declared the new Kenyan President; the claims of massive electoral frauds and cheating denounced by Ruto's rival, Raila Odinga, have been recently dismissed by the Supreme Court ruling, 5th September 2022, *Raila Odinga and others v. William Ruto and others*, Petition No. E005 of 2022. The future of the proposed Huduma Namba Bill seems to be even more complex to define in a very confused and uncertain institutional context, also following the 31st March 2022 Kenyan Supreme Court decision declaring the Building Bridges Initiative Constitutional Amendment Bill (BBI) unlawful, thus halting the proposal of a vast constitutional amendment bill able to significantly reform the Kenyan Constitution (see R. ALBERT, *Constitutional amendment and dimemberment in Kenya*, in *I-Connect Blog of the International Journal of Constitutional Law*, 21 August 2021; S. ROTHENBERGER, *The Kenyan Supreme Court writes a new chapter in the history of the rule of law in Africa*, in *I-Connect Blog of the International Journal of Constitutional Law*, 20 August 2022).

[75] At the moment writing, the proposed Huduma Namba scheme remains mandatory and will be assigned at birth or upon enrollment. Parents are required to complete the registration process of their children within 90 days after the baby's birth. Late registrations will be punished with the payment of a penalty.

[76] The ONG Article 19 Eastern Africa, in collaboration with other civil society organizations, has filed a joint memorandum to the Kenyan Parliament, asking to reform the proposed Bill. More details at https://www.article19.org/resources/consortium-calls-for-reforms-implementation-of-kenyas-digital-id/.

Moreover, alternative processes and specific guarantees in case of misfunctioning of the system or difficulties in the authentication or verification phases, leading to the denial of welfare services, are not included in the draft bill. Considering the need for data protection safeguards, NGOs and civil society representatives have underlined the absence of a fully implemented legal framework in this delicate field, claiming the need to adopt and operationalize all the regulations required by the Data Protection Act in order to entirely enforce its guarantees. For all these reasons, according to several stakeholders, the proposed bill cannot be considered as effectively transposing and fulfilling the conditions expressed by the Court's judgement[77].

The above analyzed case-law is characterized by relevant similarities, although specificities and differences are identifiable: what here interests the most is the fact that both Courts didn't deny the general legitimacy of biometric identification systems and their compatibility with recognized fundamental rights. Consequently, only specific characteristics and provisions of the impugned legislations have been affirmed as unconstitutional (e.g. the mandatory nature of the digital ID, together with the absence of a right to opt out or of alternative processes to guarantee access to vital services to those who are impeded to enroll); also the breadth of the data required for the registration revealed problematic: the proportionality and necessity test applied, led both Courts to exclude the legitimacy of a vast collection, retention and processing of a wide variety of biometric, genetic or location data. In both the examined cases the judicial litigation ultimately resulted in a push-back of the impugned provisions to national legislators and Governments, accused – even in explicit terms – of having "put the cart before the horse". The recognized negative effects and impacts on fundamental rights, clearly underlined by both Courts, need solid and comprehensive legal safeguards and guarantees in order to counterbalance the intrusion in the private sphere and the potential exclusions deriving from automated and digitalized systems. While these decisions helped prompting Governments and legislators to re-think the adopted acts, the Courts' intervention showed, at the same time, how complex the questions about proportionality and necessity of such intrusive identification systems could be and how the debate on a proper balance between efficiency and progress on the one hand and fundamental rights' protection on the other hand, remains open.

[77] See the submission presented by 12 civil society organizations, available at https://www.article19.org/wp-content/uploads/2022/01/Huduma-Bill-2021-Coalition-Submission-Jan-2022.pdf. The National Assembly has promoted several open forums to discuss the Bill and present concerns and critiques, thus involving civil society and its representatives in the legislative process.

4. Automation and Digitalization of Public Fundamental Services: The Importance of Getting It Right

Big Data, AI systems and algorithms represent important and unprecedented resources for public authorities: in the current context of progress and innovation, the digitalization of welfare states seems to be an unstoppable evolution; new technologies can undoubtedly help Governments to better serve citizens and to find new and more appropriate solutions to both emergent and historical challenges, from expenditure control of public services to lack of legal identities[78]. Accuracy, efficiency, precision and automation are key achievements, especially in the welfare sector. Nonetheless, the digital transition in such a delicate and key area of public intervention also poses enormous risks to fundamental rights, dignity and the very basis of democracy, by progressively and profoundly impacting the traditional relationship between citizens and public authorities[79].

In a rapidly evolving scenario, characterized by fast-paced technological progress, profound economic crisis, public expenditure containment policies and increasing social inequalities, the need to properly address the pressing challenges presented by the digital welfare state is more acute than ever.

The use of digital IDs obtained through the implementation of identification systems based on biometric data represents a clear example of the serious debate surrounding the adoption of digital tools in the welfare sphere. As emerged from the previous paragraphs' analysis, these sophisticated instruments can help solving deep-rooted issues, especially in developing countries facing endemic problems of poverty, corruption and inefficiency of public assistance services, also due to a vast 'un-identified' population; but, as the Jamaican and Kenyan cases have demonstrated – following the path already covered by the Indian Aadhaar scheme[80] – the Governments' favorable approach to digital transition as a way to optimize welfare services' access entails potentially disruptive effects that are mainly ignored and not properly preventively evaluated; on the contrary, civil society, academics and NGOs manifested a more skeptical approach, prompting courts' intervention and underlining drawbacks and threats, some of which vastly

[78] V. MAYER-SCHNBERGER – K. CUKIER, *Big Data. A revolution that will transform how we live, work and think*, Boston, 2013; CENTER FOR HUMAN RIGHTS AND GLOBAL JUSTICE OF THE NYU SCHOOL OF LAW, *Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID*, June 2022; R. COLLINGTON, *Disrupting the welfare state? Digitalisation and the retrenchment of public sector capacity*, in *New Political Economy*, n. 2/2022.

[79] M. TADDEO – L. FLORIDI, *How AI can be a force for good*, in *Science*, 24th August 2018; K. GALLOWAY, K., *Big Data: a case study of disruption and Government power*, in *Alternative Law Journal*, n. 42/2017; R. ANDREASSEN – A. KAUN – K. NIKUNEN, *Fostering the data welfare state: a Nordic perspective on datafication*, in *NORDICOM Review*, n. 2/2021.

[80] On this specific national biometric ID system, see *supra* (footnote n. 45) as well as S. MASIERO, *The digitalisation of anti-poverty programmes: Aadhaar and the reform of Social Protection in India*, in M. GRAHAM (ed), *Digital economies at global margins*, London, 2019.

confirmed by studies on the concrete implementation of digital IDs schemes as well as by judicial litigations' findings[81].

The described trend also receives validation in other Countries, where automated identification systems has been challenged before national judges: interesting examples can be detected not only in the Indian Aadhaar system, which continues to be highly debated and opposed even after the Supreme Court's decision[82], but also in the judicial action recently promoted in Uganda, in April 2022, by a coalition of NGOs and civil society organizations[83]: according to the applicants, the national digital ID system (the so-called Ndaga Muntu) is deemed to both violate social rights and data protection rights and to exacerbate discrimination and marginalization of the poorer and most disadvantaged[84].

But these 'side effects' of the digitalization of welfare state should not be regarded as uniquely affecting the digital transition in developing countries of the Global South: on the contrary, the specter of digital

[81] These considerations clearly emerged from the analysed case-law.

[82] After the landmark 2018 decision, briefly recalled *supra*, the Supreme Court, in the ruling *Beghar Foundation v. Justice KS Puttaswamy* of 20th January 2021, dismissed several petitions seeking the review of the previous judgment. In fact, by invoking Art. 137 of the Indian Constitution (according to which "Subject to the provisions of any law made by Parliament or any rules made under article 145, the Supreme Court shall have the power to review any judgement pronounced or order made by it"), 7 parties filed review petitions aimed at reversing the prior decision which was considered suffering from "errors apparent on the face of the record" (this is one of the conditions for review petitions required by the *Supreme Court Rules 2013* L-33004/99; for more information on the Indian Supreme Court, see, *ex multis*, M.P. JAIN, *Indian constitutional law*, New-York, 2018; D. AMIRANTE, *La democrazia dei superlativi. Il sistema costituzionale dell'India contemporanea,* Naples, 2019). These petitions were not the only ones filed after the *Puttaswamy* case: several pleas on the legitimacy and proportionality of the Aadhaar scheme have been submitted to federal as well as national courts (for example petitions concerning elections laws disciplining the Aadhaar number's linkage to voter IDs, as recalled in M. PARTHASARATHY, *Aadhaar link to voters lists. What has the Supreme Court said?*, in *Supreme Court Observer*, 21 December 2021); the persistent judicial litigation on Aadhaar project's implementation reveals the vast debate still characterizing the use of this controversial biometric IDs scheme.

[83] On this judicial litigation (*Initiative for Social and Economic Rights (ISER), Unwanted Witness (UW), and the Health Equity and Policy Initiative (HEAPI) v. Attorney General and the National Identification and Registration Authority*) as well on the functioning and characteristics of the Ndaga Muntu system, see CENTER FOR HUMAN RIGHTS AND GLOBAL JUSTICE OF THE NYU SCHOOL OF LAW, *Chased Away and Left Die. How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons*, June 2021 and the statement of ISER available at https://chrgj.org/2022/04/25/civil-society-sues-government-over-ndaga-muntu-national-id-mandatory-digital-id-threatens-lives/.

[84] More generally, in the past, the creation of mandatory 'analogic' national identity schemes based on biometric data were challenged in front of national Courts even before the implementation of sophisticated technological and automated systems: see for example the so-called Madhewoo judgement in Mauritius (*Madhewoo v. The State of Mauritius and Anor*, 2015, SCJ 177), the Judicial Yuan Interpretation No. 603 decided by the Judicial Yuan of Taiwan in 2005, the *Blas F. Ople v. Ruben Torres and Others* decided by the Philippines Supreme Court back in 1998. For more information on these cases, that rejected the legitimacy of the proposed IDs schemes, mainly due to privacy concerns, see PRIVACY INTERNATIONAL, *A guide to litigating identity systems*, cit.

divide[85] has appeared real and serious also in Europe, especially during the pandemic[86], highlighting the exclusionary risks of automated tools in the social assistance sphere. This seems to be confirmed by the high attention the creation of the Irish Public Services Card (PSC) has gained in recent years: this system, used to authenticate citizens' identity, has been adopted with the declared purpose of reducing frauds and 'welfare cheats' and has been therefore imposed as a precondition for accessing a wide range of public services, among which social welfare payments and government benefits[87]. In order to obtain the Card, applicants are demanded to provide personal information – through an interview with public authorities – and photos, processed by automated facial recognition systems and compared with other facial images retained in public databases, for the purpose of avoiding frauds and duplications. Nonetheless, the program has been vastly opposed not only by the Irish Data Protection Commission for reasons linked to the lack of transparency and of proper guarantees protecting personal and biometric data collected and retained for identity authentication[88], but also by the UN Special Rapporteur on extreme poverty and human rights; in April 2020, Alston published an official communication warning the Irish Government about the negative impacts the PSC could cause on fundamental rights and human dignity, with particular reference to the most "disadvantaged because of the bureaucratic obstacle course involved. They have to jump through a number of hoops to prove their identity, including providing

[85] As defined by the EU Parliament in December 2015 Briefing on *Bridging the digital divide in the EU*, "in 2001 the OECD defined the term 'Digital Divide' as 'the gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard both to their opportunities to access information and communication technologies (ICT) and to their use of the internet for a wide variety of activities'. Accordingly, there are two aspects to the Digital Divide: the first gap considers mainly the division between those who have access to ICT such as computers and the internet and those who do not (..) The second gap refers to different types and levels of internet use, motivation and skills". On this evolving concept, see E.M. ROGERS, *The digital divide*, in *The International Journal of Research into New Media Technologies*, n. 1/2001; T. PUCCI, *Il diritto all'accesso nella società dell'informazione e della conoscenza. Il digital divide*, in *Informatica e diritto*, n. 2/2002; L. SARTORI, *Il divario digitale: Internet e le nuove diseguaglianze sociali*, Bologna, 2006; M. FONG, *Digital divide: the case of developing countries*, in *Victoria University Issues in Informing Science and Information Technology*, n. 2/2009; E. KIM – B. LEE – N. MENON, *Social welfare implications of the digital divide*, in *Government Information Quarterly*, n. 2/2009; J. VAN DIJK, *The digital divide*, Cambridge, 2020.

[86] S. RANCHORDAS, *Automation of public services and digital exclusion*, cit.; for considerations on the impact digital divide produced during Covid-19 pandemic in different world's regions, see T. EL KADI, *Uneven disruption: Covid-19 and the digital divide in the Euro-Mediterranean Region*, in *IEMed Dossier* 2020; M. NAVARRO *et al.*, *The rural digital divide in the face of the Covid-19 pandemic in Europe*, in *Informatics*, n. 4/2020; A. RAMSETTY – C. ADAMS, *Impact of the digital divide in the of Covid-19*, in *Journal of the American Medical Informatics Association*, n. 7/2020; J. LAI – N. WIDMAR, *Revisiting the digital divide in the Covid-19 era*, in *Applied Economic Perspectives and Policy*, n. 1/2021; P. DAMIANI, *What consequences for the right to broadband internet access in rural areas of the EU?*, in *Federalismi.it*, n. 28/2021; Y. LIU – Z. FAN, *The digital divide and Covid-19. Impact on socioeconomic development in Asia and the Pacific*, in *UN ESCAP Working Papers Series*, June 2022; S. ALEXOPOULOU – J. ASTROM – M. KARLSSON, *The grey digital divide and welfare state regimes: a comparative study of European Countries*, in *Information Technology & People*, n. 8/2022.

[87] In 2020, for example, this Card was a mandatory requirement to apply for Covid-19 Unemployment Payments.

[88] See, in details, IRISH DATA PROTECTION COMMISSION, *Final investigation report in respect of the processing of personal data by the Department of Employment Affairs and Social Protection in relation to the Public Services Card*, August 2019, available at https://assets.gov.ie/69774/6d71ed5820ad42258ccfacfc9727297f.pdf.

documents which many find hard to access and attending an interview which might entail a major disruption"[89].

Similarly, the already mentioned relevant SyRI case, concerning the digital welfare fraud detection system adopted by the Dutch Government and decided by the District Court of first instance of The Hague[90], indicated the importance, also in European legal systems, to carefully evaluate the dangers deriving from automated tools, also in terms of possible discriminatory effects[91].

All these considerations lead to four conclusive remarks: the results of the analyzed case-studies on digital identity systems allow to more generally reflect on the challenges – and possible solutions – concerning digital welfare states' evolution.

First of all, the reported examples demonstrate the necessity to cautiously think about the complex relationship between law and new technologies and, consequently, to consider the role legislators and policymakers should assume. Many of the underlined issues linked to automation and digitalization are caused by the failure to apply what some scholars called a 'policy before technology' approach[92]: in other words, the approval and implementation of sophisticated yet controversial tools often fail to be preceded by a rigorous debate at the legislative level, thus limiting public participation[93] and oversight as well as transparency and accountability. What both the Jamaican and Kenyan cases clearly shows is the widespread lack of a deep prior risk assessment by public authorities, together with a poor knowledge of the technical functioning of the instruments adopted[94]: only by acknowledging the error-rates and possible malfunctioning of the digital tools intended to be implemented, it could be possible for Parliaments and Governments to enact strong, adequate and comprehensive legal frameworks and to take proactive steps to rule and prevent negative impacts and limit potential abuses. A prior assessment focusing also on the possible side effects affecting fundamental rights can help identifying pitfalls that need to be addressed before the digital schemes' concrete implementation[95]. This aspect emerges from

[89] UN Special Rapporteur on extreme poverty and human rights, *Official communication*, Reference OL IRL 1/2020, 14th April 2020, available at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25176.

[90] See *supra* footnote 17. It is interesting to recall that the case was promoted by several NGOs and that, also in this case, the UN Special Rapporteur on extreme poverty and human rights presented an *amicus* brief.

[91] In particular, this case also demonstrated that AI and algorithms systems cannot be treated as unfailing and unbiased instruments. On this point, see in particular A. RACHOVITSA – N. JOHANN, *The human rights implications of the use of AI in the digital welfare state: lessons learned from the Dutch SyRI case*, cit.; S. BEKKER, *Fundamental rights in digital welfare states: the case of SyRI in the Netherlands*, in O. SPIJKERS *et al.* (eds), *Netherlands Yearbook of International Law 2019*, Cham, 2020; S. RANCHORDAS – L. SCARCELLA, *Automated government for vulnerable citizens: intermediating rights*, in *University of Groningen Faculty of Law Research Paper*, n. 11/2021.

[92] P. DIXON, *A failure to "Do no harm"*, cit.

[93] The importance of public participation has been underlined by L. VAN ZOONEN, *Data governance and citizen participation in the digital welfare state*, in *Data & Policy*, n. 2/2020.

[94] On these aspects, see J. CANNATACI – V. FALCE – O. POLLICINO, *Legal challenges of Big Data*, London, 2020.

[95] F. PASQUALE, *The black box society. The secret algorithms that control money and information*, Cambridge, Massachusetts, 2015.

the comparative analysis of the Courts' decisions in the two examined cases as well as from other landmark judgments in similar judicial litigations[96], where Judges underlined the crucial importance of solid and comprehensive legislative provisions able to avoid violations or unproportionate restrictions of constitutionally recognized human rights.

An absent or superficial prior analysis of risks and benefits, leading to the lack of guarantees and safeguards, consequently reflects on the role played by the different Institutional actors involved in the control and implementation of the digital welfare state. In particular, the Jamaican and Kenyan case-law provides significant lessons on the relevance of Courts and civil society: these actors replaced, in some ways, the legislators' 'absenteeism'. In fact, in both Countries Judges assumed a paramount role in pressing Parliaments and Governments to halt the implementation of digital instrument, to re-consider the existent legislative framework or to adopt stronger and specific provisions regulating the challenged tools. In this sense, we can affirm that the Courts, pushed by the important civil society's action, operated *ex post* to substitute a lacking *ex ante* risk evaluation and regulatory intervention. The Courts in most of the cases, even if in different degrees, obliged legislators and policymakers to re-open the debate on the necessity and proportionality of the instruments in place, especially with regards to the guarantee of privacy, data protection and non-discrimination rights.

If the Judges' key decisions resulted in a deceleration of the digital transition in welfare services – often promoting the adoption of amendments, reforms and a stronger involvement of civil society representatives –, it cannot be ignored the 'endemic' problematic lying behind: Courts cannot be systematically seen as the sole actor able to stem the Governments' 'temptation' towards digitalization of welfare state and to ensure the respect of fundamental rights; by only limiting and mitigating already existent issues and violations, *ex post* controls cannot represent the primary and unique barrier against abuses.

The second evaluation is strictly connected to the impact the digitalization process of welfare states is causing on social equality and non-discrimination. As revealed by the examination of digital IDs systems – requiring applicants to undergo articulated procedures and to present documents (such as birth certificates) that could be difficult to obtain for certain segments of the population –, the enrollment and authentication operations often resulted in severe marginalization and exclusions: expressions such as 'digitizing discrimination' and 'automating inequality'[97] powerfully convey the threats a digital welfare state could imply, by ultimately emphasizing already existent social divisions[98]. In other words, digital

[96] For example in the recalled Indian Supreme Court decision on the Aadhaar system, in particular para. 339.
[97] V. EUBANKS, *Automating inequality: how high-tech tools profile, police and punish the poor*, cit.; see also K.K. LARSSON, *Digitization or equality: when government automation covers some but not all citizens*, in *Government Information Quarterly*, n. 1/2021.
[98] On this point L. ROBINSON *et al.*, Digital inequalities and why they matter, *Information*, in *Communication & Society*, n. 5/2015; C. O'NEIL, *Weapons of math destruction: how big data increases inequality and threatens democracy*, London, 2017; S.

instruments are capable of exacerbating forms of discrimination to the detriment of the most fragile welfare services' beneficiaries, in particular immigrants, women, elderly and poor people, especially those living in rural areas. These effects are demonstrated to be true not only with regards to digitalized identification tools but also – and more generally – with reference to other automated instruments employed in the welfare sphere, such as fraud detection tools: SyRI for example was found able to mainly affect and target vulnerable applicants living in specific areas – mainly cities' suburbs inhabited by low-income and racial minorities –[99], also opening the door to stigmatizing forms of surveillance through automated data analytics techniques[100].

If totally renouncing to innovation is not the correct answer, Governments are asked to avoid the 'digital-only' approach and to promote – as clearly stressed by the examined case-law[101] – alternative instruments for regulating the access to social assistance services, especially with reference to those who, for various reasons, result excluded from the digitalization processes; in addition, policymakers are required to boost digital inclusion through specific and publicly funded programs aiming at limiting the 'digital underclass' phenomenon[102], which will be more and more acute considering a growing aging population. As Ranchordas underlined, the fostering of digital literacy initiatives[103] and a gradual and partial shift to digitalization and automation of welfare state could be also accompanied by the recognition of a "right

THEWISSE – D. RUEDA, *Automation and the welfare state: technological change as a determinant of redistribution preferences*, in *Comparative Political Studies*, n. 2/2019.

99 As Bertolini affirmed with reference to the SyRI case, the investigations launched on the basis of the AI predictions "have proved a significant social bias by the use of variables, such as low-income households, that realise a statistical discrimination"; the author presents another relevant example of exclusionary effects deriving from digitalized welfare state's tools: the Chinese Social Credit System (SCS), defined as one of the "biggest algorithm-based rating system in the world", that "affects the welfare sector whenever the access to government subsidies, benefits and services is curtailed as a consequence for not having carried out either a court order or an administrative decision or whenever an individual does not behave properly", E. BERTOLINI, *Is technology really inclusive?*, cit., p. 9.

100 See S. ZUBOFF, *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, London, 2019. On this point, "Jorgensen states the DWS is being implemented in an asymmetric power scheme, whereby the authorities can access data more than the citizens who own them. Excessive access to data can be used by authorities to monitor and predict the behavior of citizens, thus becoming a basis for discrimination and stigmatization. This asymmetric power structure represents the new order of colonialism – which has been called data colonialism – in which humans are being normalized through data for the benefit of the data owners", Z. LARASATI – T.K. YUDA – A.R. SYFA'AT, *Digital welfare state and problem arising*, cit., p. 2, recalling R.F. JØRGENSEN, *Data and rights in the digital welfare state: the case of Denmark*, in *Information Communication and Society*, n. 1/2021.

101 As already underlined in the previous paragraph, the need to provide different and alternative systems and processes able to guarantee access to fundamental services to those excluded from the automated and digitalized programmes as well as opt-out alternatives have been clearly declared by both the Jamaican and Kenyan Courts.

102 F. MANJOO, *The tech industry is building a vast digital underclass*, in *New York Times*, 24th July 2019.

103 According to the UNESCO, digital literacy is "the ability to access, manage, understand, integrate, communicate, evaluate and create information safely and appropriately through digital technologies for employment, decent jobs and entrepreneurship. It includes competences that are variously referred to as computer literacy, ICT literacy, information literacy and media literacy", UNESCO, *A Global Framework of Reference on Digital Literacy*, Information Paper N. 51/2018, UIS/2018/ICT/IP/51, p. 4. See also T. DOBSON – J. WILLINSKY, *Digital literacy*, in D.R. OLSON – N. TORRANCE (eds), *The Cambridge handbook of literacy*, Cambridge, New York, 2009; W. EICHHORST – U. RINNE, *Digital challenges for the welfare state*, in *IZA Policy Paper*, n. 134/2017; P. REDDY *et al.*, *Digital literacy: a review of literature*, in *International Journal of Technoethics*, n. 2/2020.

to make a mistake", that entails "the adoption of policies or legislative measures that promote administrative leniency towards citizens who are not digitally literate"[104]. Such an approach reveals opposite to one followed by several implemented digital welfare tools which, on the contrary, oblige welfare services' beneficiaries to bear the costs of legal assistance necessary to prove they didn't act with the manifest purpose of defrauding public authorities or, alternatively, the correctness of the data submitted[105].

These considerations lead to a strictly linked additional remark, concerning, more specifically, the impact of privacy-invasive instruments on the very functioning of welfare systems: in fact, by imposing citizens to 'trade' their unique and sensitive data, intimately connected to their identity[106], and to 'give up' the control over their personal information as the only way to obtain access to vital welfare services, public authorities create intrusive instruments, able to surveil, target and also punish beneficiaries[107]. This ultimately drives to a ubiquitous surveillance[108] that affects not only privacy and data protection but also the role attributed to public actors in our democratic societies: citizens applying for public assistance are not to be considered suspects but first and foremost rights-holders[109]; this simple principle, that should govern the relationship between citizens and public authorities, risks to be overwhelmed by new technologies such as automated frauds detection instruments and biometric identification systems which are based, on the contrary, on the idea that applicants must be controlled and surveilled to guarantee efficiency and costs-savings. As a consequence, the burden of accountability is shifted uniquely on citizens, who could find it enormously difficult and expensive to defend, assert and prove their rights[110].

---

[104] S. RANCHORDAS, *Automation of public services and digital exclusion*, cit. and of the same author *Administrative vulnerability and digital technology: a novel concept for inclusive administrative law*, in *I-Connect Blog of the International Journal of Constitutional Law*, 11th November 2020.

[105] V. GANTCHEV, *Data protection in the age of welfare conditionality: respect for basic rights or a race to the bottom*, in *European Journal of Social Security*, n. 1/2019.

[106] Especially when unique and irreplaceable biometric data are involved.

[107] M.H. MURPHY, *Algorithmic surveillance: the collection conundrum*, in *International Review of Law, Computers and Technology*, n. 2/2017.

[108] Using a vivid expression employed by Z. BAUMAN, D. LYON, *Liquid surveillance. A conversation*, Cambridge, 2012.

[109] As affirmed by R.F. JØRGENSEN, *Data and rights in the digital welfare state: the case of Denmark*, cit., "the digital welfare state will advance a digital technocracy that treats its citizens as data points suited for calculation and prediction rather than as individuals with agency and rights", p. 1. On this point, see also J. STORM PEDERSEN, *The digital welfare state: dataism versus relationshipism*, in J. STORM PEDERSEN – A. WILKINSON (eds), *Big Data. Promise, applications and pitfalls*, London, 2019 and L. DENCIK, *The datafied welfare state: a perspective from the UK*, in A. HEPP – J. JARKE – L. KRAMP (eds), *New perspectives in critical data studies. The ambivalence of data power*, Cham, 2022, who affirms that "Rather than the state being accountable to its citizens, the datafied welfare state is premised on the reverse, making citizens' lives increasingly transparent to those who are able to collect and analyse data, at the same time as knowing increasingly little about how or for what purpose that data is collected", p. 157.

[110] In 2008, Agamben, talking about identification and control systems requiring tourists and visitors' fingerprints at the airport, stated that "what is at stake is none other than the new and 'normal' biopolitical relation between citizens and the State. This relation no longer has to do with free and active participation in the public sphere but instead concerns the routine inscription and registration of the most private and incommunicable element of subjectivity. The State has made the citizen into the suspect par excellence", G. AGAMBEN, *No to Biopolitical Tattooing*, in *Communication and Critical*

This worrying scenario appeared evident not only in the SyRI case, in which individuals targeted by the automated analysis as 'at risk of fraud' were obliged to strive for proving the system wrong – with significant difficulties also due to the lack of transparency on how the AI worked[111] – but also in the Jamaican, Kenyan and Indian cases, where citizens who weren't able to have their identities authenticated by the automated biometric identification system or to provide all the documents necessary to enroll, had no – or very limited – ways to see their social rights recognized.

The last consideration originates from the examined case-law and regards the relevant role played by the comparative analyses: the Jamaican Court, in its decision, openly and extensively quoted the landmark dissenting opinion expressed by Indian Supreme Court Justice Chandrachud in the Aadhaar case[112]; the Kenyan Court recalled the Indian decision on similar automated welfare tools, while all Courts made references to the Canadian and USA jurisprudence as well as to the historical ECtHR case-law concerning the guarantee of privacy and data protection rights in front of sophisticated yet invasive technological systems. Notwithstanding the relevant differences between the examined legal systems and the USA and European legal traditions – the latter being characterized by strong and well-established guarantees of privacy and data protection rights, while the formers have a limited and recent judicial and legislative experience in this field –, the reasoning followed by the Jamaican and Kenyan Judges reveals an in-depth and profound reflection on the risks and effects of the welfare state's digital transition. The proposed balancing between different rights and interests at stake could, in conclusion, be beneficial for every Country – developing Countries but also Western democracies – interested or on its way to implement digital tools in the welfare sphere.

The detailed and extensive investigation of the delicate public debate as well as of the complex judicial litigations derived from the selected cases must encourage legislators, courts, civil society and academics to keep in great attention and raise awareness on the ongoing digital evolution of welfare assistance.

As suggested by Solove, a metaphor different from the widely used Orwellian Big Brother seems to be more appropriate to describe the threats caused by massive automation and digitalization of public decisions and services: that of the Kafka's masterpiece 'The Trial'. Similarly to what happened to Josef, an alarming menace is nowadays to be identified in the creation of an indifferent, automated and

Cultural Studies, n. 2/2008. Similarly on the concept of 'biopower', it has been underlined that "The power to identify has frequently been framed as the power to subdue: Amoore argues that biometrics used on a mass scale tend to facilitate 'the exercise of biopower such that the body itself is inscribed with, and demarcates, a continual crossing of multiple encoded borders – social, legal, gendered, racialized and so on'", A. MARTIN – L. TAYLOR, *Exclusion and inclusion identification: regulation, displacement and data justice*, cit., p. 50.

[111] Individuals that have their benefits suspended "fail either to know whether the investigation or the suspension was launched following a false positive [the systems notifying individuals as possible fraud perpetrators erroneously] or which data justified the launching of the investigation or the suspension of the benefits", E. BERTOLINI, *Is technology really inclusive?*, cit., p. 9.

[112] See *supra* footnote n. 51.

dehumanized public administration and bureaucracy[113], in front of which citizens and, more specifically, applicants for welfare assistance feel vulnerable, surveilled, under suspicion and left without accessible ways to control and oppose the functioning and outcomes of automated or 'by default' decisions[114].

Prior risk assessment, comprehensive legislative frameworks, civil society involvement in decision-making and regulatory processes, careful *ex-post* controls and digital literacy policies could help preventing this worrying scenario.

[113] Bertolini speaks about the risk of 'human authority' being progressively replaced by 'digital authority' (E. BERTOLINI, *Is technology really inclusive?*, cit.).

[114] This metaphor is also recalled by Karel De Gucht in the preface of S. GUTWIRTH *et al.* (eds), *Reinventing data protection?*, Berlin, 2009, p. vi.