doi:10.1017/aju.2023.21

SYMPOSIUM ON CRITICAL INTERNATIONAL LAW AND TECHNOLOGY

AUTOMATING RACIALIZATION IN INTERNATIONAL LAW

*Priya S. Gupta**

From the continuation of colonial power structures in global economic development institutions,[1] to immigration policies that favor applicants from white-majority European countries,[2] to the use of counter-terrorism law to target primarily Muslim people,[3] international law and its domestic analogues reflect and further inscribe racial distinctions and hierarchies. Racialization in international law occurs in the more visible areas of public decision making but also in mundane, administrative practices. In this essay, I argue that digital technologies are at the heart of automating processes of racialization in international law. Digital technological instruments effectively divide the global population, decision by decision, in adherence to the logics of racial hierarchy: they distribute social and material rights and privileges through financial, welfare, and immigration decisions while simultaneously deepening and entrenching state surveillance, policing, and violence.

International law enacts a *double opacity* which shields multiple automations of racialization from scrutiny and accountability: first, in its blindness to the systemic and mutually reinforcing nature of racial disparity and relatedly, in the use of proxies for race such as geography, facial features, or wealth; second, in its promulgation and protection of digital technology as a *purportedly neutral* arbiter of myriad public and private decisions, hiding bias in technical complexity, corporate secrecy, and intellectual property protection, and across jurisdictional lines.

"Racialization" and Digitalization in International Law

The ongoing inscription of racial categorization by law—"racialization"—is an active process that does not respond to a reality, but rather, summons one. It divides and hierarchizes the global population into categories of differential social and material treatment based on race. Race, in turn, draws socially determined distinctions of the global population based on perceived phenotype and ancestry.[4] Dressed up as "biological," these distinctions were promulgated during colonialism and conquest and continue today to inform a differentiated,

* *Associate Professor, McGill University Faculty of Law, Montreal, Canada.* Thank you to Neha Jain, Fleur Johns, Benedict Kingsbury, Frédéric Mégret, Gregor Noll, Galit Sarfaty, and Peer Zumbansen for insightful comments and conversations.

[1] Sundhya Pahuja, Decolonising International Law: Development, Economic Growth and the Politics of Universality (2011).

[2] E. Tendayi Achiume, *Racial Borders*, 110 Geo. L.J. 445 (2022).

[3] Fahid Qurashi, *The Prevent Strategy and the UK "War on Terror": Embedding Infrastructures of Surveillance in Muslim Communities*, 4 Palgrave Comm. 1 (2018).

[4] *See generally* Ian F. Haney-López, *The Social Construction of Race: Some Observations on Illusion, Fabrication, and Choice*, 29 Harv. C.R.-C.L. L. Rev. 1 (1994); Marilyn Lake & Henry Reynolds, Drawing the Global Colour Line: White Men's Countries and the Question of Racial Equality (2008).

local-global architecture of securitization and surveillance, entrenched and normalized in quotidian social as well as administrative practices.

Racial discrimination is prohibited by a number of human rights instruments, including the Universal Declaration of Human Rights, the International Convention on the Elimination of All Forms of Racial Discrimination, the Inter-American Convention Against Racism, Racial Discrimination and Related Forms of Intolerance, and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Under the International Convention on the Elimination of All Forms of Racial Discrimination, bringing a claim requires showing discriminatory conduct that has an identifiable harm.[5] Gathering evidence and proving such a claim presents significant challenges for individual claimants. What this (already imperfect) system of accountability misses, however, are *sets of practices* that are not clearly delineable as single acts that may result in individual harms as well as cumulative, aggregate reinforcement of racial disparities.

The use of digital technologies in international legal decision making multiplies those "sets of practices" across areas, reinforcing structural racism while at the same time making it more difficult to identify and seek recourse. Digital technologies include the use of "big data" (exceptionally large amounts of personal and other information), the analysis of this data through algorithms executed by artificial intelligence (AI), and automated decision making. These decisions govern sensitive and consequential areas of life—areas that have also long been marked by racial inequality. It remains a challenge to locate the intentionality of an algorithm's racial bias. The use of proxies for race or the triangulation of large data sets, including countless visual images and demographic and geographic location data, perpetuates the production of racially discriminatory outcomes. Impactful racial bias becomes a function of machines' processing of vast, continuously expanding data sets, which are collected, voluntarily offered, or silently "scraped" from personal devices.[6] Amongst academic, government, and industry-based calls for the greater use of AI to eradicate bias in decision making, there is growing evidence and extensive acknowledgement in legal scholarship that racial, gender, and ability-based discrimination is embedded in decision-making processes that are based on machine learning and algorithms.[7] The remainder of this essay illustrates the automation of racialization in four areas of international law: border control; surveillance; military and policing; and finance, before turning to the issue of democratic accountability.

Border Control

International borders are inherently racial, whereby whiteness allows for "mobility and migration."[8] As Tendayi Achiume argues, colonial histories of explicit racial inclusion and exclusion have evolved into "facially race-neutral legal categories and regimes of territorial and political borders (sovereignty, citizenship, nationality, passports, and visas)" and "rules and practices of national membership and international mobility," which nonetheless are encoded with racial privilege.[9] Decisions at the border may not be made on explicitly racial grounds, but rather on proxies such as place or name which in effect enact a racial division, protected by a superficial neutrality (the first opacity).

[5] On how "racial discrimination" in human rights focuses on acts rather than ideology, see Anna Spain Bradley, *Human Rights Racism*, 32 HARV. HUM. RTS. J. 1 (2019).

[6] VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018).

[7] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016); Anya E. R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 IOWA L. REV. 1257 (2020).

[8] Achiume, *supra* note 2.

[9] *Id.* at 449.

https://doi.org/10.1017/aju.2023.21 Published online by Cambridge University Press

AI further cloaks those racially based decisions through its purported neutrality and "black box" procedural intransparencies (the second opacity). Digital technologies play multiple roles in today's "smart" borders. "Lie-detecting" automated bots using AI are being tested as border control decisionmakers.[10] Residency applications are processed automatically in some jurisdictions, as are determinations of someone's "security risk," welfare benefits, and document verification.[11] Cameras, computers, fingerprint readers, and body scanners extract data from people even before they arrive at borders. In Europe, data extracted from personal devices is "weaponized to undercut" asylum claims—a practice which is impermissible against its own citizens.[12] Biometrics analysis of physical characteristics (facial recognition, fingerprint recognition, hand geometry, iris and retina recognition) and of behavioral characteristics (voice and handwriting recognition) is being rapidly expanded around the world.[13]

Surveillance

Public surveillance regimes racialize societies by targeting those of a particular race, national origin, or religion depending on the context. The United Kingdom, the United States, and Canada each have programs which surveil Muslim people within their respective borders.[14] The United States has long had programs surveilling Black citizens, including those involved with the Civil Rights Movement or Black Lives Matter.[15] Real-time facial recognition is used during peaceful protests by local police units while massive amounts of surveillance data are collected in secrecy.

Private surveillance and data collection through social media, insurance companies, employers, and security, health devices, and household items (the "Internet of Things") adds to the complexity of regulation. Even where much of that data is collected with informed consent, the device user's inability to control the fate of their data has prompted heightened disillusionment among data privacy scholars concerning consent-based, contractual data governance. Complicating matters and blurring public and private here are ongoing questions about access to data by police and the criminal justice system.[16]

Both public and private surveillance raise crucial questions as to international law's treatment of race. First, how can the International Convention on the Elimination of All Forms of Racial Discrimination's commitment to "eliminating racial discrimination in all its forms" in Article 2 and the freedoms protected in Article 5(d), including (i) movement, (iv) thought, conscience and religion, (viii) opinion and expression, (ix) peaceful assembly and

[10] Umberto Bacchi, *EU's Lie-Detecting Virtual Border Guards Face Court Scrutiny*, REUTERS (Feb. 5, 2021); European Commission CORDIS, Intelligent Portable Border Control System: iBorderCtrl Project Fact Sheet; Hannah Tyler, *The Increasing Use of Artificial Intelligence in Border Zones Prompts Privacy Questions*, MIGRATION POL'Y INST. (Feb. 2, 2022).

[11] Derya Ozkul, *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe*, REFUGEE STUD. CTR. (2023).

[12] E. Tendayi Achiume, *Digital Racial Borders*, 115 AJIL UNBOUND 333 (2021).

[13] KAREN FOG OLWIG, KRISTINA GRÜNENBERG, PERLE MØHL & ANJA SIMONSEN, THE BIOMETRIC BORDER WORLD: TECHNOLOGY, BODIES AND IDENTITIES ON THE MOVE (2021); Simone Browne, *Digital Epidermalization: Race, Identity and Biometrics*, 36 CRITICAL SOC. 131 (2010); AYELET SHACHAR, THE SHIFTING BORDER: LEGAL CARTOGRAPHIES OF MIGRATION AND MOBILITY (2020); Dimitri van den Meerssche, *Virtual Borders: International Law and the Elusive Inequalities of Algorithmic Association*, 33 EUR. J. INT'L L. 171 (2022).

[14] Sabrina Alimahomed-Wilson, *When the FBI Knocks: Racialized State Surveillance of Muslims*, 45 CRITICAL SOC. 871 (2019); Qurashi, *supra* note 3; Colleen Bell, *Surveillance Strategies and Populations at Risk: Biopolitical Governance in Canada's National Security Policy*, 37 SEC. DIALOGUE 147 (2006).

[15] Eyako Heh & Joel Wainwright, *No Privacy, No Peace: Urban Surveillance and the Movement for Black Lives*, 3 J. RACE, ETHNICITY & CITY 121 (2022); KENNETH O'REILLY, RACIAL MATTERS: THE FBI'S SECRET FILE ON BLACK AMERICA, 1960–1972 (1991); Toppa Mudassar & Princess Masilungan, *Struggle for Power: The Ongoing Persecution of Black Movement by the U.S. Government*, MOVEMENT 4 BLACK LIVES (2021).

[16] Ángel Diaz, *When Police Surveillance Meets the "Internet of Things,"* BRENNAN CTR. JUST. (2020).

https://doi.org/10.1017/aju.2023.21 Published online by Cambridge University Press

association, be met if the violations and evidence of aggregate, coordinated racial targeting are often secret and under the cover of "security"? Second, how can international law recognize the structural disenfranchisement and deterrence from participation in public life resulting from a collective abridgement of multiple rights? Finally, how can data sharing for racialized surveillance between transnational companies and states be regulated?

Military and Policing

Digital technologies in military activities and policing include the use of real-time facial recognition, involuntary personal data extraction through stingray and digital receiver technology, drones, high-definition streaming-enabled cameras, the militarization of equipment and tactics,[17] and predictive policing and automated criminal justice procedures.[18] These technology-enabled methods are highly racialized, deployed against Black people in the United States, Palestinians in the West Bank and Gaza, and Latin American migrants traveling north.[19] This targeting of racialized groups affect a panoply of rights, from the ones referred to above, as well as the International Convention on the Elimination of All Forms of Racial Discrimination's right to equal participation in cultural activities in Article 5(e)(vi) and the right of access to public places and services in Article 5(f).

Technology-enabled racialized targeting is often based on collaboration between states. As reported by a number of organizations, notably Amnesty International, the United States has some of its local police units train with security forces in Israel, sharing tactics from racial profiling to "crowd control" weapons and surveillance technology.[20] The United States has trained local police across the world for over a century, including in techniques involving increased militarization and technology.[21] If a state violates its own citizens' human rights, questions (should) arise in international law with regard to: the state that provided the training and technology for such violations; the technology hardware and software companies; and, the authors of the facial recognition and other surveillance algorithms.

Finance

Financial decisions from insurance to investment, consumer credit, and mortgages are made based on the collection of data and the algorithmic analysis of risk. Decentralized finance (DeFi) enables lenders and borrowers to cross jurisdictional lines. It has been lauded as inclusionary because of the anonymity and geographic diversity of borrowers, purportedly avoiding identity-based discrimination that lenders are known for.[22] Yet as the Bank for International Settlements notes, the reliance on borrower *collateral* in lieu of identifying information restricts lending to the already asset-rich, in effect "negating financial inclusion benefits."[23]

[17] Stop LAPD Spying Coalition, *The Architecture of LAPD Surveillance* (2014).

[18] Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. ONLINE 15 (2019).

[19] Amnesty International, *Automated Apartheid: How Facial Recognition Fragments, Segregates and Controls Palestinians in the OPT* (2023); Mizue Aizeki, Laura Bingham & Santiago Narváez, *The Everywhere Border. Digital Migration Control Infrastructure in the Americas*, TRANSNAT'L INST. (Feb. 14, 2023).

[20] Mersiha Gadzo, *How the US and Israel Exchange Tactics in Violence and Control*, AL JAZEERA (June 12, 2020); Edith Garwood, *Where Do Many Police Departments Train? In Israel*, AMNESTY INT'L USA (2016).

[21] JEREMY KUZMAROV, MODERNIZING REPRESSION: POLICE TRAINING AND NATION-BUILDING IN THE AMERICAN CENTURY (2012); Gustavo A. Flores-Macías & Jessica Zarkin, *The Militarization of Law Enforcement: Evidence from Latin America*, 19 PERSPEC. POL. 519 (2021).

[22] FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2016).

[23] Sirio Aramonte, Sebastian Doerr, Wenqian Huang & Andreas Schrimpf, *DeFi Lending: Intermediation Without Information?*, 57 BANK FOR INT'L SETTLEMENTS (2022).

https://doi.org/10.1017/aju.2023.21 Published online by Cambridge University Press

Hidden racism in lending algorithms through DeFi or the use of traditional credit scores may be perpetuated by private actors, but is enabled by a paucity of domestic and international regulation. The paucity of regulation, in particular international fair lending regulation, implicates Article 2.1(b) of the International Convention on the Elimination of All Forms of Racial Discrimination obligating states "not to sponsor, defend or support racial discrimination by any persons or organizations"; Article 2.2, committing states to take "concrete measures" to guarantee racialized persons "the full and equal enjoyment of human rights and fundamental freedoms"; and Article 5 which affirmatively commits states to "prohibit and to eliminate racial discrimination in all its forms and to guarantee . . . equality before the law" including with respect to the right to property.

Democratic Accountability?

International law is a crucial battleground for the regulation of systemic racial biases wrought by digital technologies. Given the power imbalances embedded in international law, critical scholarship from global administrative law to Third World Approaches to International Law has long challenged Global North-centric conceptions of sovereignty, legitimacy, and accountability. What does the exercise of such significant power not just by non-state actors, but non-human, automated ones, do to standard conceptions of state power in the international realm, upon which these conventions were based?[24] This is not the first time non-state power and agency have challenged classic international legal structures, but digital technologies present radically new forms and processes of that power, evading a system largely built around individual acts and individualized accountability: the "who" has transformed, the racial disparities are systemic, and individual rights-based systems of justice are increasingly inadequate both domestically and internationally.

Automated decision making decenters the previous preoccupation with the "who" of transnational governance and the concern over its legitimacy shifts attention to the "how."[25] The traditional concern with holding a particular actor accountable risks running empty in light of the difficulty of attaining and mobilizing actionable evidence of racial discrimination for a successful claim. The key question—namely who authored, who implemented, and who scrutinizes (the decision suggested by) the algorithm—is the subject of considerable debate.[26] The "author" of the code may not be the *agent* behind its meaning or its discriminatory impact.[27] Moreover, legal challenges to discriminatory decisions made by algorithms are often stymied by intellectual property and corporate secrecy protections.

Part of the challenge in eradicating systemic racial disparities wrought by digital technologies is that these technologies often do their worst damage under the surface. What they really do is not what they say they do—for example, in a world of immense amounts of personal data on mobile phones, the interruption of human circulation at the border or in public space is not merely about preventing passage but rather slowing it to enable extraction and thereby, governance.[28] Holding either public or private actors accountable becomes increasingly difficult as traditional notions of acts and agency fail to capture who (or what) is doing what, and with what intentions and effects.

[24] Fleur Johns, *International Law and the Provocations of the Digital: The 2021 Annual Kirby Lecture in International Law*, 40 AUSTRL. Y.B. INT'L L. ONLINE 3 (2022).

[25] THE POLITICS OF TRANSNATIONAL GOVERNANCE BY CONTRACT (A. Claire Cutler & Thomas Dietz eds., 2017); Fleur Johns, *Governance by Data*, 21 ANN. REV. L. & SOC. SCI. 53 (2021).

[26] Katharina Pistor, *Statehood in the Digital Age*, 27 CONSTELLATIONS 3 (2020).

[27] LOUISE AMOORE, CLOUD ETHICS: ALGORITHMS AND THE ATTRIBUTES OF OURSELVES AND OTHERS (2020).

[28] *See* Louise Amoore, *Biometric Borders: Governing Mobilities in the War on Terror*, 25 POL. GEOGRAPHY 336 (2006); Polly Pallister-Wilkins, *How Walls Do Work: Security Barriers as Devices of Interruption and Data Capture*, 47 SEC. DIALOGUE 151 (2016).

https://doi.org/10.1017/aju.2023.21 Published online by Cambridge University Press

The weakness of rights-based systems to scrutinize, review, and resist automated decision making is deeply accentuated in the international context, which must grapple with activities of both public and private actors across jurisdictional lines and regulatory regimes, mechanisms of judicial action which depend on the plaintiff to gather evidence of bias, and the inadequacy of existing transparency efforts in the face of massive data complexity and volume.

Conclusion

Digital technologies accelerate the demarcation of racial hierarchies by enabling it in more spheres of life and through more inequality-perpetuating decisions, thereby unleashing negative, networked consequences which remain protected by the rhetorics of technology and neutrality. What is at stake here is not just accountability for individual discriminatory acts, but rather democratic accountability for opaque methods of racial societal ordering from migration and mobility, to participation in public space and freedom from arbitrary imprisonment, as well as material allocations.

Did we really think that people—prejudiced by race, gender, sexual orientation, age, disability, national origin, language, religion, caste, and a multitude of other perceived distinctions—could build neutral decision-making factories, run by machines? That we could substitute their "judgment" (i.e., calculated outcomes) for our collective reasoning, and that we would end up with justice? *Who* built those machines? *Whose values* were encoded and invisibilized?

https://doi.org/10.1017/aju.2023.21 Published online by Cambridge University Press