NOTES

AI AT THE BORDERS: HOW THE EU AI ACT CAN PROVE TO BE INCOMPATIBLE WITH FUNDAMENTAL RIGHTS FOR REFUGEES

Ahmad Ibsais*

Abstract

With the emergence and growing sophistication of artificial intelligence (AI), there is a new set of challenges at the intersection of innovation, fundamental human rights law, and migration policy within the European Union (EU). This Note critically examines the EU's approach to AI regulation, particularly its application at borders and in migration contexts, following the signing of the EU AI Act of 2024. The current framework risks undermining fundamental rights guaranteed by the EU Charter of Fundamental Rights. The AI Act, while a step towards AI governance and future jurisprudence, contains loopholes and exemptions for border control. Thus, within the context of refugees and asylum seekers, the AI Act may serve to exacerbate discrimination.

The exemption for border control risks setting a precedent that undermines migrant rights and human dignity through its biometric data collection, data transfers, and predictive analytics that can be used to target individuals based on race, religion, and nationality. At the same time, EU member states claim to be leaders in ethical AI development and deployment. By exploring relevant case law, current practices, and regulatory frameworks, the paper examines the debate within EU jurisprudence on surveillance, data collection, security, and data protection.

This Note (1) analyzes the EU AI Act in relation to the Charter of Fundamental Rights of the EU (CFREU), looking to rights to privacy, asylum, and non-discrimination; (2) examines the interplay between national security and rights of refugees when AI-surveillance and data collection is used; (3) critiques AI in migration management; and (4) proposes reforms to ensure AI use at borders aligns with the CFREU.

[*] Ahmad Ibsais is a Palestinian American and third-year law student at the University of Michigan Law. He is a writer at Al Jazeera and a freelance writer for various outlets including The Guardian, CNN, and The Nation. He previously served as a fellow at the Marion B. Brechner First Amendment Law Project and was named one of Arab-America Foundation's 30 under 30. © 2025, Ahmad Ibsais.

I. INTRODUCTION

In 2015, the European Union's (EU) refugee crisis began with the arrival of over one million refugees—primarily from Syria, Afghanistan, Iraq, and various African nations—who were seeking safety within EU borders from persecution, war, and economic hardship.[1] The influx of migrants, many being of Arab and African descent, led to significant changes in EU border controls, policies, and technologies.[2] The EU accelerated its use of artificial intelligence (AI) and automated decision-making systems at its borders to help with acquiring, storing, and analyzing data.[3] This AI technology, while facially neutral, risks amplifying the already discriminatory practices against future marginalized populations seeking refuge.[4]

Throughout the last decade, this emergence of AI has manifested in different forms, from emotion detection systems in Hungary, Greece,

[1] Linda Peters et al., *Explaining Refugee Flows. Understanding the 2015 European Refugee Crisis through a Real Options Lens,* 18(4) PLOS ONE, 1 (2023).

[2] *See* Petra Molnar, *Technology on the Margins: AI and Global Migration Management from a Human Rights Perspective*, 8 CAMBRIDGE INT'L L.J. 305, 314-18 (2019).

[3] For a recent report mapping the large range of new technologies, including AI, applicable at borders, arrival and after arrival in Europe, see generally DERYA OZKUL, AUTOMATING IMMIGRATION AND ASYLUM: THE USES OF NEW TECHNOLOGIES IN MIGRATION AND ASYLUM GOVERNANCE IN EUROPE (2023).

[4] Ludivine Sarah Stewart, *The Regulation of AI-Based Migration Technologies Under the EU AI Act: (Still) Operating in the Shadows?*, 30 EUR. L.J. 122, 123 (2024).

and Latvia, to software that can detect dialects for asylum procedures in Germany.[5] The deployment of AI technology does not happen in isolation, but is instead a part of the rapidly expanding AI ecosystem that uses analytics methods such as biometric data capture and automated risk assessments, all of which create a discriminatory impact on asylum applications.[6] Since AI systems in asylum processing are fundamentally designed to mirror existing human judgment patterns, they risk codifying and systematizing the same prejudices and flawed reasoning that may already exist in traditional decision-making frameworks.[7] The AI ecosystem's limited oversight in screening asylum applications, coupled with the exemptions that apply to the European Union's AI use in migration, creates tension with the rule of law. This tension impacts the accountability and transparency of government(s) and its actions, most importantly when fundamental rights are involved.[8] The unprecedented expansion of AI technology has occurred without the necessary public scrutiny or oversight;[9] the lack of oversight in the AI Act leads to the concern of this Note: the EU AI Act's disregard for the fundamental rights of vulnerable migrant populations.

The European Parliament approved the AI Act on March 13, 2024, making the AI Act the first in the world to comprehensively regulate AI with fundamental rights protections in mind.[10] While the EU posits itself as a leader in ethical AI governance, this Note will instead argue that the AI Act's intention and potential effect are in contradiction. Although AI used in the migration context is considered "high risk," given that the use of AI would require special oversight due to the potential to invade one's rights, the AI Act's loopholes and exemptions may undermine the rights in the EU Charter, specifically as they relate to privacy rights which may be violated through broad data

[5] *Id.* at 122; Ozkul, *supra* note 3, at 43-48.

[6] *See EU Entry/Exit System Might Be Delayed Again*, ETIAS (Sept. 26, 2024), https://etias.com/articles/eu-entry/exit-system-might-be-delayed-again (discussing the use biometric technology being used to collect data without supported infrastructure).

[7] *See e.g.*, Amina Memon et al., *Artificial Intelligence (AI) in the asylum system.* 64 MED. SCI. & L. 87, 87-90 (2024) (discussing UK's use of AI in asylum credibility assessment).

[8] *See* Ellis Paterson & Gemma McNeil-Walsh, *Catching up with the Debate: Artificial Intelligence & the Rule of Law*, RECONNECT (Oct. 14, 2019), https://reconnect-europe.eu/blog/aiandrolpatersonmcneilwalsh/.

[9] *See e.g.*, Petra Molnar & Sarah Chander, *The AI Act: EU's Chance to Regulate Harmful Border Technologies*' THOMSON REUTERS FOUND. (May 17, 2022), https://news.trust.org/item/20220518062025-xfh8g/(discussing various AI technologies employed at the borders and their impact to marginalized communities).

[10] European Parliament Press Release IPR 19015, Artificial Intelligence Act: Parliament Adopts Landmark Law (Mar. 13, 2024).

capture.[11] Member states are bound to employ existing EU legislation when using AI, such as data protection; however, the AI Act includes exemptions such as "security," which will allow member states to use increasingly invasive AI tools like iBorderCtrl[12] and Automated Virtual Agent for Truth Assessment in Real-time[13] (AVATAR) at borders. Both iBorderCtrl and AVATAR are control systems that use AI to detect deception by analyzing facial expressions or through other means of automation.[14] However, these systems lack scientific validity, vary based on cultural context, and have discriminatory impact with high false positives.[15] The use of interoperable systems, like European Asylum Dactyloscopy Database (EURODAC) and European Travel Information and Authorization System (ETIAS), implements extensive surveillance structures that, using the AI Act's exemptions, can target certain migrant populations; EURODAC, for instance, collects, stores, and transfers fingerprint data.[16]

Beyond technical implementation, the issues with AI border technologies also extend to accountability. For instance, the AI Act nominally prohibits real-time remote biometric identification in certain spaces, with an exception for law enforcement and border agents, these effectively hollow out the protections for migrant populations and can be used to collect information unknowingly or to unfairly deny their asylum applications.[17] Furthermore, the existence of the AI Act's exemptions could

[11] *See* Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689) 1, ¶ 60 [hereinafter EU AI Act]; *id., Annex III: High Risk Systems Referenced in Article 6(2)*, https://artificialintelligenceact.eu/annex/3/; *id*, art. 6.

[12] Umberto Bacchi, *EU's Lie-Detecting Virtual Border Guards Face Court Scrutiny*, THOMSON REUTERS FOUND. (Feb. 5, 2021), https://www.reuters.com/article/technology/eus-lie-detecting-virtual-border-guards-face-court-scrutiny-idUSL8N2KB2GT/.

[13] *See* AARON C. ELKINS ET AL., APPRAISING THE AVATAR FOR AUTOMATED BORDER CONTROL: RESULTS OF A EUROPEAN UNION FIELD TEST OF THE AVATAR SYSTEM FOR INTERVIEWING AND PASSPORT CONTROL CONDUCTED AT THE HENRI COANDĂ INTERNATIONAL AIRPORT, BUCHAREST, ROMANIA (2013).

[14] *See id.* at 3; Bacchi, *supra* note 12; EU AI Act art. 2(3).

[15] *Automated technologies and the future of Fortress Europe*, AMNESTY INT'L (Mar. 28, 2019), https://www.amnesty.org/en/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe/.

[16] Anilya Krishnan, *The Dark Side of EURODAC*, REGUL. REV. (Oct. 24, 2023), https://www.theregreview.org/2023/10/24/krishnan-the-dark-side-of-eurodac/.

[17] *Packed with Loopholes: Why the AI Act Fails to Protect Civic Space and the Rule of Law*, EUR. CTR. FOR NON-FOR-PROFIT L. (Apr. 3, 2024), https://ecnl.org/news/packed-loopholes-why-ai-act-fails-protect-civic-space-and-rule-law, ("While the Act requires AI developers to maintain high standards for the technical development of AI systems (e.g. in terms of documentation or data quality), measures intended to protect fundamental rights, including key civic rights and

lead to criminalizing migration, which conflicts with refugee rights that the EU has already established.

Without transparency and accountability, and in light of the procedural obstacles for migrants seeking remedy in situations where AI at borders violated their rights, the protections that the AI Act aims to establish in the realm of AI are illusory. Thus, the Note proceeds as follows: Part II examines the legal foundation of the AI Act and its reliance on Article 114 TFEU; Part III investigates current AI technologies deployed at EU borders and demonstrates how these practices potentially violate fundamental rights; Part IV focuses on the specific provisions of the EU's Charter of Fundamental Rights that may be at risk, including the right to privacy; finally, Part V puts forward reforms to strengthen the trustworthy objective the AI Act aims to achieve.[18] At the moment, the AI Act can be used to ignore one's fundamental rights like asylum, privacy, and protection of data through its exemptions that will indirectly lead to discrimination based on race, religion, and nationality.[19] The dignity of migrants and ethical considerations cannot be sacrificed at the altar of innovation.

II. Legal Basis for the EU AI Act

The AI Act was signed by the European Commission as a Regulation as opposed to a Directive, since a Regulation confers supremacy and direct applicability across member states.[20] In the Commission's 2020 Proposal to harmonize rules on artificial intelligence, the Commission defends its choice of the instrument, reasoning that "the choice of a regulation as a legal instrument is justified by the need for a uniform application of the new rules."[21] Adopting a Regulation establishes direct applicability to the member states under Article 288 of the Treaty on Functioning of the European Union (TFEU), which states that "a regulation shall have general application. It shall be binding in its entirety and directly applicable in all member states."[22] In doing so, the goal is to prevent member states from implementing their divergent rules on AI governance,

freedoms, are insufficient to prevent abuses. They are riddled with far-reaching exceptions, lowering protection standards, especially in the area of law enforcement and migration.").

[18] *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021) [hereinafter *Commission Proposal*].

[19] *See* Charter of Fundamental Rights of the European Union, arts. 1, 21, 2012 O.J. (C 326) 396, 400. [hereinafter CFREU] (establishing binding protections that may be undermined by broad exemptions in the AI Act).

[20] EU AI Act, *supra* note 11.

[21] *Commission Proposal*, *supra* note 18, ¶ 2.4.

[22] Consolidated Version of the Treaty on the Functioning of the European Union of 26 Oct. 2012, art. 288, 2012 O.J. (C 326) 47.

which might create more liability and inconsistencies in AI frameworks that could remove more fundamental rights. Furthermore, the use of a regulation also created immediate legal force once the AI Act was finally signed. Established in *Costa*, the EU regulations became part of the national legal system without the need for states to implement legislation.[23] The use of a regulation also means that enforcement powers are clear for EU members: the AI Act's provisions can be invoked before any EU member's national courts by states or by EU citizens impacted by AI systems against the EU.[24] Migrants who are EU nationals could invoke the EU AI Act as infringing on their rights, but these same rights may not extend to refugees who are more vulnerable when crossing into the EU.[25]

The EU AI Act relies primarily on Article 114 of the TFEU, which authorizes measures "for the approximation of provisions . . . which have as their object the establishment and functioning of the internal market."[26] Grounding the AI Act in Article 114 is emblematic of the EU's focus on prioritizing harmonization of the internal market. The Commission uses Article 114 of the TFEU to argue that variations in AI regulation across Member States would fragment the market.[27] This approach, however, leaves communities vulnerable to heightened surveillance. The Commission attempts to remedy the limitations of Article 114 by employing Article 16 both for supplemental authority and to address personal data protection, stating that "everyone has a right to the protection of personal data concerning them" and "rules relating to the protection of individuals with regard to the processing of personal data . . . and the rules relating to the free movement of such data" must be established.[28]

[23] Case C-6/64, Costa v. ENEL, ECLI:EU:C:1964:66, ¶ 3 (July 15, 1964).

[24] *See* Case C-26/62, Van Gend v. Neth. Inland Revenue Admin., ECLI:EU:C:1963:1 (Feb. 6, 1963).

[25] *See* Joint Statement, Amnesty International, Joint Statement: The Future EU Must Uphold the Right to Asylum in Europe (July 9, 2024), https://www.amnesty.org/en/latest/research/2024/07/joint-statement-the-future-eu-must-uphold-the-right-to-asylum-in-europe/#:~:text=Attempts%20to%20outsource%20asylum%20to,have%20served%20as%20a%20warning ("Outsourcing asylum processing and protection to third countries who cannot provide effective protection or are already disproportionately hosting refugees, is inconsistent with the objective and spirit of the Refugee Convention. It also obfuscates jurisdiction and responsibility, making it more difficult for people to access justice when their rights are violated. Where extraterritorial asylum processing has been tested, it has caused immeasurable human suffering and rights violations.").

[26] Consolidated Version of the Treaty on the Functioning of the European Union, art. 114(1) of May 9, 2008, 2008 O.J. (C 115) 94 [hereinafter TFEU].

[27] European Parliament, Resolution of 20 Oct. 2020 with Recommendations to the Commission on a Civil Liability Regime for Artificial Intelligence, 2021 O.J. (C 404) 107.

[28] TFEU, *supra* not 26, at art. 16.

At first glance, it seems that the supplemental legal basis strengthens the AI Act's rights framework; however, it is limited practically by the broad exemptions for border controls under "national security" objectives. "National security" is not clearly defined within EU law, with significant variation in how the term is interpreted by member states, leading to concerns about where the lines should be drawn between what is and is not excluded from the AI Act. The European Court of Justice (ECJ) tried to interpret national security in *Johnston,* national security being the narrow exception to fundamental rights, justified only when specific and proportionate to security needs .[29] While *Johnston* dealt with gender discrimination in Northern Ireland's police force, its principles can be applied to the national security exemptions in the AI Act.[30] There, the court emphasized that any degradation from fundamental rights on the grounds of national security must be strictly interpreted and "within the limits of what is appropriate and necessary for achieving the aim in view."[31] This is particularly relevant to border control exemptions in the AI Act. *Johnston* put forth instances in which national security could be used: (1) proportionate to the legitimate aim pursued;[32] (2) based on objective criteria; and (3) subject to effective judicial review.[33] This framework can be used in the AI Act's context so that member states cannot invoke broad security justification that would discriminate against refugees and asylum seekers. However, the current formulation of the AI Act lacks the safeguards of *Johnston*, which requires an individualized assessment of security needs, not general security concerns.[34] Currently, the AI Act permits broad exemptions for border control systems with limited human oversight that do not mention individual assessment.[35]

[29] *See* Case C-222/84, Johnston v. Chief Constable of the Royal Ulster Constabulary, ECLI:EU:C:1986:206 (May 15, 1986).

[30] *Id.*

[31] *Id.* at ¶ 38.

[32] *Id.* at ¶ 32.

[33] *Id.* at ¶ 60, ("Article 2 (2) of Directive No. 76 allows a Member State to take into consideration the requirements of the protection of public safety in a case such as the one before the Court,". 'Public Safety' is considered an objective criteria).

[34] *Id.* at ¶ 38; James Clark et al., *Europe: The EU AI Act's Relationship with Data Protection Law: Key Takeaways, Privacy Matters*, DLA PIPER (Apr. 25, 2024), https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/ (This article discusses the interplay between the EU AI Act and the General Data Protection Regulation (GDPR), highlighting that the GDPR's broad definition of "processing" encompasses activities conducted on personal data, including data storage, thereby applying to AI systems where personal data is involved.)

[35] EU AI Act, *supra* note 11, recital 130, https://artificialintelligenceact.eu/recital/130/("It is thus appropriate that under exceptional reasons of public security or protection of life and

In 2020, the Court of Justice of the European Union (CJEU) tried to formally define national security as a responsibility that "encompasses the prevention and punishment of activities capable of seriously destabilizing the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities."[36] With the AI Act broadly framing "national security," the real-time implication on asylum seekers and refugees from backgrounds that have historically been discriminated against in the EU cannot be understated.[37]

III. AI Technologies at EU Borders: Current Practices and Possible Rights Violations

While the AI Act's legal foundation focuses on market harmonization, its practical implications can have damaging effects. The AI Act creates specific exemptions for law enforcement, explicitly "to detect, prevent, investigate and prosecute criminal offenses" and provides exemptions from obligations to inform individuals about their interaction with AI systems.[38] This exemption extends to generative and manipulative AI, making it nearly impossible to challenge discriminatory applications.[39] Since these exemptions are not clearly defined in the context of border control, their implications on fundamental rights will be damning given that border agents are a policing force. Moreover, refugees face considerable challenges in directly accessing the ECJ as they lack direct standing to bring cases before the ECJ unlike EU citizens.[40]

Current border practices have demonstrated entrenched patterns of discrimination against refugees and asylum seekers from Middle Eastern and African nations.[41] These patterns emerge in discriminatory

health of natural persons, environmental protection and the protection of key industrial and infrastructural assets, market surveillance authorities could authorise the placing on the market or the putting into service of AI systems which have not undergone a conformity assessment.").

[36] Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net v. Premier Ministre, ECLI:EU:C:2020:791, ¶ 135 (Oct. 6, 2020).

[37] *See, e.g.*, Press Release, European Union Agency for Fundamental Rights [EUFRA], Muslims in Europe face ever more racism and discrimination (Oct. 24, 2024), https://fra.europa.eu/en/news/2024/muslims-europe-face-ever-more-racism-and-discrimination.

[38] EU AI Act, *supra* note 11, at art. 50(1).

[39] *Id.* at art. 50(4).

[40] TFEU, *supra* note 26, art. 263 ("[a]ny natural or legal person may, under the conditions laid down in the first and second paragraphs, institute proceedings against an act addressed to that person or which is of direct and individual concern to them.")

[41] OJEAKU NWABUZO & LISA SCHAEDER, RACISM AND DISCRIMINATION IN THE CONTEXT OF MIGRATION IN EUROPE, 3 (2017).

processing, violence, and denial of rights.[42] AI systems trained on this history, as is the case of the EU AI Act, will only amplify these violations.

Data from multiple sources show discriminatory practices at EU Borders: there have been thousands of reported pushback incidents per the Border Violence Monitoring Network between 2019 and 2022;[43] studies show asylum seekers from Muslim backgrounds face higher rejection rates than those not of Muslim origins at EU borders[44] and there is a high rejection rate for African asylum seekers in Melilla and Ceuta.[45] The Temporary Protection Directive (TPD) was made to provide immediate protection for displaced people internal and external to the EU.[46] However, the TPD has been applied selectively as it was used to help Ukrainian refugees in 2022, but not in 2015 to Syrian refugees facing a similar humanitarian crisis.[47]

Moreover, the pattern of selective policies at EU borders is further reinforced by the EU AI Act, which specifically violates the Charter of Fundamental Rights of the EU (CFREU) through its biometric identification at the borders, expansive data collection, limited transparency, data storage & sharing, automated decision-making, and risk assessment systems.[48] The AI Act defines biometric data in Article 3(34) as "personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images."[49] The technology being used to capture this data will be used to disproportionately impact Muslim migrants; in fact, investigations revealed that companies based in France, Sweden, and the

[42] *Id.* at 17-22; *How European Policies Choose Violence Against Migrants and Refugees*, DOCTORS WITHOUT BORDERS (Mar. 14, 2024), https://www.doctorswithoutborders.org/latest/how-european-policies-choose-violence-against-migrants-and-refugees.

[43] BORDER VIOLENCE MONITORING NETWORK, BLACK BOOK OF PUSHBACKS (2022).

[44] Kirk Bansak et al., *How Economic, Humanitarian, and Religious Concerns Shape European Attitudes Toward Asylum Seekers*, 354 SCIENCE 217, 218 (2016).

[45] *See* Michelle Furrer, *Rejections at the Border: Concerning Patterns in the United States and European Union Asylum Policies, a Comparative View of the United States' Title 42 Policy and Spain's Pushbacks in Ceuta and Melilla*, MITCHELL HAMLINE L. REV. AMICUS CURIAE BLOG (Jan. 28, 2023), https://mhlawreview.org/amicus-curiae/rejections-at-the-border-concerning-patterns-in-the-united-states-and-european-union-asylum-policies-a-comparative-view-of-the-united-states-title-42-policy-and-spains-pushbacks-in/.

[46] Council Directive 2001/55, 2001 O.J. (L 212) 12 (EC).

[47] Eric Reidy, *What the EU's Policy Toward Ukrainians May Mean for Other Refugees*, NEW HUMANITARIAN (Apr. 21, 2022), https://www.thenewhumanitarian.org/analysis/2022/04/21/what-the-EUs-policy-toward-ukrainians-may-mean-for-other-refugees.

[48] *See* Bacchi, *supra* note 12; Elkins et al., *supra* note 13, at 3.

[49] EU AI Act, *supra* note 11, at art. 3(34).

Netherlands sold their digital surveillance systems to Chinese mass surveillance apparatuses to be used against Uyghurs, a Turkic ethnic group that is primarily Muslim.[50] This comes at a time when nearly one in two Muslims in the EU face discrimination daily, a rise from a 2016 report.[51] In Greece, the use of their Centaur AI system has come under heavy criticism for violating fundamental rights in its disproportionate deployment in areas with high Syrian refugee populations.[52] The Centaur system utilizes AI behavioral analytics, drone monitoring, and thermal detection systems to detect threats automatically.[53] Centaur works in tandem with Hyperion to collect and store fingerprint data to facilitate movement with refugee camps filled with Syrian and Afghani refugees.[54]

While Article 5(1)(h) of the AI Act nominally restricts real-time biometric identification and data storage, the exceptions instead authorize this form of surveillance for both the "prevention of a specific, substantial, and imminent threat" and the "detection, localization, identification, or prosecution of a perpetrator or suspect."[55] Since border control falls under the broad exemption for security, and storage for such data can be indefinite, it is unclear how biometric data can be used against refugees once they matriculate in the EU. For instance, the United States collected biometric data against Afghan citizens during its invasion following 9/11.[56] This data was stored, with no reference to specific time frames, without legitimate purposes, and subsequently used against Afghan civilians.[57] After the United States left Afghanistan in 2021, this data was never erased, and the Taliban was able to use this U.S. stored biometric data against its own people for nefarious purposes.[58] Iran also used biometric data, in the form of facial recognition, to track and arrest women who

[50] *EU Companies Selling Surveillance Tools to China's Human Rights Abusers*, AMNESTY INT'L (Sept. 21, 2020), https://www.amnesty.org/en/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers/.

[51] EUFRA, *supra* note 37.

[52] Lydia Emmanouilidou & Katy Fallon, *With Drones and Thermal Cameras, Greek Officials Monitor Refugees*, AL JAZEERA (Dec. 24, 2021), https://www.aljazeera.com/news/2021/12/24/greece-pilots-high-tech-surveillance-system-in-refugee-camps.

[53] Lydia Emmanouilidou, *Greek Data Watchdog To Rule on AI Systems in Refugee Camps*, PULITZER CTR. (Oct. 30, 2023), https://pulitzercenter.org/stories/greek-data-watchdog-rule-ai-systems-refugee-camps.

[54] *Id.*

[55] EU AI Act, *supra* note 11, at art. 5(1)(h).

[56] Eileen Guo & Hikmat Noori, *This is the real story of the Afghan biometric databases abandoned to the Taliban*, MIT TECH. REV. (Aug. 30, 2021), https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/.

[57] *Id.*

[58] Ken Klippenstein, *The Taliban Have Seized U.S. Military Biometric Devices*, THE INTERCEPT (Aug. 17, 2021), https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/.

defied their mandatory hijab law.[59] Thus, the question remains: can indefinite retention and indiscriminate collection of biometric data happen at EU borders without violating fundamental rights of asylum seekers? If not, how can their data be used once asylum seekers make their way into the EU?

Furthermore, the AI Act does not address algorithmic bias, which produces results reflecting already existing biases in society based on current historical and social inequalities.[60] As it relates to border control, the effects of AI may be clearer: higher rejection for certain demographics, flagging certain demographics more often, and capturing or misusing data from certain demographics in ways that violate their fundamental rights. However, the AI Act's impact at the intersection of law enforcement and border control has more room for thought. For instance, with AI border technologies, there are several challenges: (1) the exemptions enable authorities to collect biometric data; (2) broad surveillance under "security" is not necessary or proportional; and (3) the technology's uses do not align with fundamental rights.

The widespread data capture and storage allowed under these exemptions can be used against refugee populations, in conflict with existing jurisprudence like *S. and Marper v. United Kingdom.*[61] In *Marper,* the European Court of Human Rights (ECtHR) found that indefinite retention of personal data violated the plaintiff's rights to privacy (Article 7) and right to protect personal data (Article 8).[62] There, the claimants had their DNA and other biometric data taken during arrest and U.K. authorities refused to destroy the samples.[63] U.K. law allows indefinite data retention of DNA regardless of conviction.[64] The court said that retaining data (i.e., fingerprints, DNA profiles, and biometric data) without consent or reason was a disproportionate interference

[59] *Iran Installs Cameras to Find Women Not Wearing Hijab*, BBC NEWS (Apr. 8, 2023), https://www.bbc.com/news/world-65220595; Halley Ott, *Iran Electronically Surveilling Women to Find Headscarf Violations, U.N. Report Says*, CBS NEWS (Mar. 14, 2025) https://www.cbsnews.com/news/iran-electronically-surveilling-women-headscarf-violations-un-report-warns/ ("At Tehran's Amirkabir University, authorities installed facial recognition software at its entrance gate to also find women not wearing the hijab").

[60] Lakshitha R Jain & Vineetha Menon, *AI Algorithmic Bias: Understanding its Causes, Ethical and Social Implications*, 2023 IEEE 35TH INT'L CONF. ON TOOLS WITH A.I. (ICTAI) 460, 460, 467 (2023).

[61] *See* S. & Marper v. United Kingdom, Apps. Nos. 30562/04 and 30566/04, ¶ 19 (Apr. 12, 2008), https://hudoc.echr.coe.int/fre?i=001-90051 (discussing retention for "purposes related to the prevention or detection of crime").

[62] *Id.* at ¶¶ 67, 68, 103.

[63] *Id.* at ¶¶ 9-13.

[64] *Id.* at ¶ 13.

with one's Article 7 and 8 rights.[65] The EU AI Act allows for biometric data retention under the national security exemption, but as discussed later, the exemption is unjustified based on current, publicly accessible information that discusses how refugees do not inherently bring crime to Europe.[66] Thus, the retention of data from those seeking refuge in the EU would disproportionately interfere with their data and privacy rights.

The AI Act also creates a strong likelihood of indirect discrimination, which is prohibited in EU jurisprudence. In *D.H. and Others,* the ECtHR looked into indirect discrimination.[67] There, the Czech Republic's school system engaged in discrimination against Roma students by placing disproportionate numbers in "special schools."[68] The school system was not explicitly discriminatory, but its intelligence tests did not consider cultural differences.[69] The Court ruled that seemingly neutral provisions can still be discriminatory if they disproportionately harm a certain group.[70] This case provides another lens through which to examine indirect discrimination in the AI Act and how it is applied at EU borders. The *D.H.* Court, while not laying out a formal test, found that "neutral" policies can be discriminatory if: (1) a particular harm has occurred or is likely to occur, (2) the harm manifests or is likely to manifest significantly within a group of protected peoples, and (3) the harm is disproportionate.[71] The Czech government argued that there was an objective reason since they used psychological tests to determine intelligence to place students, but the court rejected this argument.[72] Discriminatory intent is not required for indirect discrimination if statistical evidence shows a disproportionate impact against protected groups.[73]

[65] *Id.* at ¶ 119. ("the Court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken – and retained – from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected.").

[66] *See infra* notes 97-99.

[67] *See generally* D.H. and Others v. Czech Republic, App. No. 57325/00, (Nov. 13, 2007), https://hudoc.echr.coe.int/fre?i=001-83256.

[68] *Id.* at ¶¶ 77-80, 142-144, 197.

[69] *Id.* at ¶¶ 199-201.

[70] *Id.* at ¶ 194 (citing ¶ 184).

[71] *Id.* at ¶¶ 184-85, 188, 191, 195-96, 207.

[72] *Id.* at ¶¶ 144-166, 200-201.

[73] *Id.* at ¶ 188.

Similarly, EU courts should reject future litigation that broad security exemptions are objective when there is no data to back up indiscriminate data collection. The implication for discrimination in the AI Act's implementation at the borders is clear when discrimination is already occurring against minority populations and the AI Act does not provide any structure for oversight. The broad "security" objectives will be used to embed systemic discrimination if it is anything like current practices. The predicted measurable harm(s) will be the increased detention, secondary screening, and higher rejection rates of targeted ethnic groups—those of African, Middle Eastern, and/or Muslim origins—and the disproportionate effect will be assumed to be greater than it is currently. Through the AI Act's exemptions, indirect discrimination is likely to take place against populations even though no objective aim is pursued.

IV. AI Act's Inconsistency with EU Law

A. *How the AI Act violates provisions from the Charter of Fundamental Rights*

The following part of this Note examines how current practices violate specific sections of the CFREU and other legal mediums in the EU. While designed to protect fundamental rights, the EU AI Act contains exemptions that do not guarantee those rights to vulnerable communities, rights that are guaranteed under the CFREU. The analysis below includes specific provisions of the AI Act, coupled with documented discrimination, which creates its own framework to violate CFREU rights.

1. Right to Privacy (Article 7)

The Right to Privacy (Article 7) proclaims that "everyone has the right for his or her private and family life, home, and communications."[74] In the case of *Digital Rights Ireland*, the ECJ emphasized that a limitation on one's right to privacy must be "precisely circumscribed by provisions to ensure that it is limited to what is strictly necessary" when they invalidated the Data Retention Directive.[75] The Data Retention Directive allowed internet service providers to retain extensive metadata on communications from their users.[76] The goal of the directive

[74] CFREU, *supra* note 19, at art. 7.

[75] Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, ECLI:EU:C:2014:238, ¶ 65 (Apr. 8, 2014).

[76] *See* Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of

was to support law enforcement in investigating serious crimes.[77] In its ruling, the ECJ held that data retention must be proportionate to the objective pursued and that indiscriminate retention exceeds what is necessary.[78] This is particularly important in the case of the AI Act, whose exemptions are broadly defined in border contexts, allowing for surveillance and data capture and retention on grounds of "national security."[79] The exemption makes way for indiscriminate data retention that is not proportionate to security needs, because data is collected without individual assessment. Migrants' personal data is collected and stored regardless of whether there is a specific reason for doing so, such as a prior criminal conviction.[80] Without clear objectives, the discrimination happening at EU borders against refugees and internal migrants may be magnified by the loopholes in the AI Act.[81] In *Huber*, the processing of personal data happened against migrants, who were nationals of a member state, when Germany maintained the personal data of an Austrian national, but not of its citizens.[82] The plaintiff argued that this practice of storing data of only non-German EU nationals infringed upon non-discrimination rights, the right to free movement, and the right to privacy.[83] The Court agreed, finding data retention to be discriminatory and incompatible with EU Law.[84] *Huber* helps to show that the protection against AI data capture and retention will be applied equally to EU nationals (migrants and citizens).

Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 57 [hereinafter Data Retention Directive].

[77] *See generally* Data Retention Directive 2006/24/EC.

[78] Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, ECLI:EU:C:2014:238, ¶ 46 (Apr. 8, 2014).

[79] EU AI Act, *supra* note 11, at ¶ 24.

[80] *Id.* at Recital 24 ("If, and insofar as, AI systems are placed on the market, put into service, or used with or without modification of such systems for military, defence or national security purposes, those should be excluded from the scope of this Regulation regardless of which type of entity is carrying out those activities, such as whether it is a public or private entity."); ¶¶ 38-40 (discussing exception related to criminal conviction).

[81] *See* Oxfam Int'l International, *At Europe's Borders, Migrants and Refugees Are Denied Their Basic Human Rights* (Apr. 5, 2017), https://www.oxfam.org/en/europes-borders-migrants-and-refugees-are-denied-their-basic-human-rights; European Union Agency for Fundamental Rights, Investigations of Rights Violations at EU Borders Remain Ineffective (July 30, 2024), https://fra.europa.eu/en/news/2024/investigations-rights-violations-eu-borders-remain-ineffectivehttps://fra.europa.eu/en/news/2024/investigations-rights-violations-eu-borders-remain-ineffective.

[82] Case C-524/06, Huber v. Bundesrepublik Deutschland, Opinion of Mr. Advocate General Poiares Maduro, ECLI:EU:C:2008:724, ¶ 1 (Apr. 3, 2008).

[83] *Id.* at ¶ 4.

[84] *Id.* at ¶ 32.

However, the question remains as to whether non-EU refugees will have the same protections if "security" is invoked. Furthermore, while the court recognized fighting crime as a legitimate reason for data collection,

> [F]ighting crime requires the systematic processing of personal data of EU citizens but not of that relating to nationals. This would be tantamount to saying that EU nationals pose a greater security threat and are more likely to commit crimes than citizens, which, as the Commission points out, is completely unacceptable.[85]

As discussed further below, statistical evidence does not show that refugee communities pose a crime risk to Europe, making the excuse of fighting crime moot in a refugee's right to privacy.

2. Non-Discrimination Principle (Article 21)

The principle of nondiscrimination is enshrined in Article 21 of the CFREU, which states that "any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief" shall be prohibited.[86] The principle of nondiscrimination covers both direct and indirect discrimination.[87] In *Razpredelenie Bulgaria AD (CHEZ)*, the Court distinguished between direct and indirect discrimination: direct discrimination occurs where one "person is treated less favourably than another is, has been or would be treated in a comparable situation on grounds of racial or ethnic origin;"[88] whereas indirect discrimination "is to be taken to occur where an apparently neutral provision, criterion or practice would put persons of a racial or ethnic origin at a particular disadvantage compared with other persons, unless that provision, criterion or practice is objectively justified by a legitimate aim."[89] In *CHEZ,* an energy company installed electricity meters at an inaccessible height in certain neighborhoods populated with Roma communities.[90] The Court held that the practice was direct discrimination, even though the claimant was not of

[85] *Id.* at ¶ 21.

[86] CFREU, *supra* note 19, at art. 21.

[87] *Id.* at art. 21(2) ("any discrimination on grounds of nationality shall be prohibited.").

[88] Case C-83/14, CHEZ Razpredelenie Bulgaria AD v. Komisia za zashtita ot diskriminatsia, ECLI:EU:C:2015:170, ¶ 2 (Mar. 12, 2015).

[89] *Id.* at ¶ 89.

[90] *Id.*at ¶ 21.

Roma origin, under the Racial Equality Directive (Directive 2000/43/EC) as a certain group became particularly disadvantaged.[91] Placing the meters high, even if it applied to all residents in the area, was direct discrimination as it targeted a specific ethnic group.[92]

In the AI Act, discrimination can occur both directly and indirectly. As it applies to direct discrimination, similar to *CHEZ* where discrimination was direct even when "combining with other grounds,"[93] the exemptions in the AI Act would directly target certain migrant communities based on historical demographic data on refugee flow and data on pushbacks from EU borders. Just because discrimination might occur against other ethnic groups (such as Ukrainian migrants following the Russian invasion) does not negate the primary impact against migrant groups of Arab and African origins.[94] Indirectly, discrimination will occur, as the communities impacted by the AI technology will be those from Arab, African, and Muslim-majority countries, even though the provision's exemptions appear to be neutral and not specific to those of certain backgrounds. The AI technology can engage in predictive policing and detection software that is skewed toward certain groups.[95] So, if even the AI Act's exemption is considered facially neutral in the context of border policing, it results in disadvantages for refugee communities (based on refugee statistics in the EU, these communities are from Syria, Iraq, Afghanistan, and various African nations).[96] In *CHEZ,* the particular disadvantage was that Roma communities would be unable to access electricity meter readings.[97] Here, the AI Act could lead to impacted communities having higher rates of secondary screenings, longer processing times, more visa denials, more entry

[91] Case C-83/14, CHEZ Razpredelenie Bulgaria AD v. Komisia za zashtita ot diskriminatsia, ECLI:EU:C:2015:480, ¶ 75-76 (July 16, 2015).

[92] *Id.* at ¶ 31.

[93] *Id.* at ¶ 82.

[94] *Id.* at ¶ 75.

[95] *See, e.g.,* EU AI Act, *supra* note 11, art. 5(1)(d); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) art 4(4) [hereinafter GDPR] (prohibiting AI systems that assess the likelihood of a person committing a crime based solely on profiling or personality traits, but allowing use where "objective and verifiable facts" already link the person to criminal activity, a vague standard that may still enable predictive policing under the guise of "supporting" human judgment).

[96] See also Peters, *supra* note 1 (identifying Syria, Iraq, Afghanistan, and Eritrea as origin countries for the refugee seeking asylum in Europe in 2015).

[97] Case C-83/14, CHEZ Razpredelenie Bulgaria AD v. Komisia za zashtita ot diskriminatsia, ECLI:EU:C:2015:480, ¶¶ 8, 60 (July 16, 2015).

rejections, and presumptions of "national security" threats based on one's ethnicity.

As mentioned in *CHEZ,* indirect discrimination is permissible if it is "objectively justified by a legitimate aim."[98] Under the AI Act, a discriminatory exemption is permitted under "national security," which would be its "legitimate aim."[99] However, broadly surveilling refugees at EU borders should not be accepted to be legitimate. While the data varies between EU countries and refugee-origin countries, several studies show little correlation between refugee populations and increased violent crime rates in Europe.[100] In 2015, the European Social Survey, using individual-level data on victimization, found that immigrants do not have a high effect on crime.[101] In the U.K., the arrival of asylum seekers in the late 1990s and early 2000s had no measurable effect on violent crime rates.[102] Additionally, Dreher et al. found that migration from Muslim-majority countries is not systematically associated with more terrorism.[103] Furthermore, an Ordinary Least Squares regression (OLS) model, using data from 2008-2019 in Germany, found "no significant association between the change in the current share of immigrants and the change in the total crime rate."[104] Lastly, a report by the French government's Center for International Prospective Research and Data shows that when biases and overrepresentations are eliminated, "studies unanimously conclude there is no impact of immigration on crime."[105] Legitimate aims must be based on facts, not biases, and the facts do not support the AI Act's exemptions.[106]

[98] *Id.* ¶ 54.

[99] EU AI Act, *supra* note 11, art. 2(3) ("This Regulation does not apply to areas outside the scope of Union law, and shall not, in any event, affect the competences of the Member States concerning national security, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences.")

[100] *See infra* note 101, 1278 ("There was no effect on violent crime; arrest rates were not different, and changes in crime cannot be ascribed to crimes against immigrants")

[101] Luca Nunziata, *Immigration and Crime: Evidence from Victimization Data*, 28 J. POPULATION ECON. 697, 700-701 (2015).

[102] Brian Bell et al., Crime and Immigration: Evidence from Large Immigrant Waves, 95(4) REV. ECON. AND STAT., 1278 (2013).

[103] Axel Dreher et al., *The Effect of Migration on Terror: Made at Home or Imported from Abroad?*, 53 (4) CAN. J. ECON., 1703 (2020).

[104] Rita Maghularia & Silke Uebelmesser, *Do Immigrants Affect Crime? Evidence for Germany*, 211 J. ECON. BEHAV. AND ORG., 486, 488 (2023).

[105] Arnaud Philippe & Jérôme Valette, I*mmigration et DRDélinquance: Réalités et Preceptions* [*Immigration and Deliquency: Realities and Perceptions*], 436 LA LETTRE DU CENTRE D'Études Prospectives et d'Informations Internationales [Ctr. for Prospective Stud. and Int'l Info.] (Apr. 2023) 1, 1 (Fr.).

[106] *Necessity & Proportionality*, EUR. DATA PROT. SUPERVISOR, https://www.edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en (last visited Mar. 24, 2024).

Notwithstanding the question of legitimate aims as it applies to the AI Act, actions taken in pursuit of a legitimate aim must be "necessary" and "proportionate."[107] Proportionality "requires that advantages due to limiting the right are not outweighed by the disadvantages."[108] The nature of the exemptions to target migrant communities, are overbroad and do not target specific threats.[109] The harm to these communities may face should outweigh the speculative security benefits that are not grounded in fact. Border security is a legitimate aim, but alternative measures can be taken that do not trample upon the rights of those seeking refuge: individual risk assessments, cooperating with countries of origin, evidence-based security, and specified use for data collection and retention. Until the AI Act adopts a rights-informed approach to AI surveillance and data use, in pursuit of an objective aim, it will violate the nondiscrimination principle.

3. Protection of Personal Data (Article 8)

Article 8 of the CFREU affirms for everyone the right to the protection of personal data concerning them, requiring that data be "processed fairly for specified purposes on the basis of consent . . . or some other legitimate basis laid down by law."[110] The ECJ has held, several times, that mass surveillance procedures shall be limited in scope and pursuant to a specified objective.[111] In the *La Quadrature du Net* series of cases, the ECJ held that EU law precluded national legislation requiring providers of communication services to carry out indiscriminate transmission of location data to security and intelligence agencies for national security.[112] The Court said that such retention was only warranted in cases where there was a serious threat, and the nature of the measure must be "strictly" proportionate.[113] Currently, the AI Act's exemptions enable expansive surveillance. The surveillance that can be

[107] CFREU, *supra* note 19, art. 52. ("Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union").

[108] *Id.*

[109] *See* Medlir Mema, *The EU AI Act: Two Steps Forward, One Step Back* (Mar. 19, 2024), https://www.globalgovernance.eu/publications/the-eu-ai-act-two-steps-forward-one-step-back.

[110] CFREU, *supra* note 19, art. 8.

[111] *See generally* Case C-83/14, CHEZ Razpredelenie Bulgaria AD v. Komisia za zashtita ot diskriminatsia, ECLI:EU:C:2015:170 (Mar. 12, 2015).

[112] Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net v. Premier ministre, ECLI:EU:C:2020:6, ¶¶ 155, 168 (Oct. 6, 2020).

[113] *Id.* at ¶¶ 14, 125.

conducted against migrants is indiscriminate as it obtains and indefinitely retains biometrics, surveillance, and other data against all at EU borders without serious threat. The AI Act's broad data capture, without an objective serious threat, should be limited in scope, so as to not violate the personal data rights of those individuals who do not actually pose a national security threat. Currently, the AI Act is not "strictly" proportional. As previously noted, the AI Act must comply with previous case law and defined rights, such as *Digital Rights Ireland* and *Huber v. Germany*.[114] These protections for personal data clearly extend to EU nationals, but not so clearly to refugees and non-EU migrants seeking refuge within the EU due to the aim of national security.

4. Right to Asylum (Article 18)

Article 18 of the CFREU specifies that "the right to asylum shall be guaranteed with due respect for the rules of the Geneva Convention."[115] This right is also affirmed and supported by the principle of non-refoulement under Article 19(2), which would prohibit returning an asylum seeker to their country if they would face prosecution.[116] The right to asylum cannot be compromised by criminal proceedings;[117] where the court held that asylum cannot be revoked on the ground that one has been convicted of a crime without individual consideration;[118] where the ECJ ruled that the refusal of an asylum application for an Ivorian national who was convicted of a crime was improper. From preliminary legal analysis, the AI Act may not directly be used to arrest refugees at the EU borders, or upon entry, but the legislation's loopholes will aid in discriminatory practices against refugees like profiling and surveillance. In turn, this may lead to the detention of refugees whose asylum claims should be further insulated from the detentions resulting from the discriminatory practices. Even so, the use of AI analysis, with largely automated processing exempt from human review, to facilitate arrests of vulnerable people is an affront to their human dignity, which is solidified both in the CFREU and the U.N. Charter of Rights.[119]

[114] *See* Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, ECLI:EU:C:2014:238 (Apr. 8, 2014); Case C-524/06, Huber v. Bundesrepublik Deutschland, Opinion of Mr. Advocate General Poiares Maduro, ECLI:EU:C:2008:724, (Apr. 3, 2008).

[115] CFREU, *supra* note 19, at art. 18.

[116] *Id.* at art. 19(2).

[117] *See* Joined Cases C-391/16, C-77-77 and C-78/17, M v. Minsterstvo Vnitra, ECLI:EU:C:2018:486 (June 21, 2018).

[118] *Id.* at ¶¶ 132-134.

[119] G.A. Res. 217 (III) A, Universal Declaration of Human Rights, pmbl. (Dec. 10, 1948); CFREU, *supra* note 19, at art. 1 ("Human dignity is inviolable.")

B. *(In)Consistency with Other EU Statutes*

1. General Data Protection Regulation

The exemptions in the AI Act are in tension with the General Data Protection Regulation (GDPR) of the EU. First, Article 5(1)(a) of the GDPR requires that personal data be processed "lawfully, fairly, and in a transparent manner in relation to the data subject."[120] Transparency is fundamental to data rights. However, there is a carve-out in the AI Act that challenges this principle of transparency: Article 49(4) requires high-risk systems in border management to be registered in non-public sections of the EU database.[121] This exemption reflects member states prioritizing data capture.[122] Since data collection, storage, and use happen in a private setting, the protection of personal data afforded in typical public spaces will not apply to refugees at EU borders.[123]

Second, Article 5(1)(b) of the GDPR defines the scope of purpose mandating that data be "collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[124] Generally, the AI Act accounts for this provision. Article 10 of the AI Act states that there should be "appropriate data governance and management practices," which would include data collection.[125] However, as the Platform for International Cooperation on Undocumented Migrants (PICUM) points out, the exemptions in the AI Act might allow for broader data collection and will be used, provided it is invoked under "any matters of migration, policing, and security."[126] This creates a parallel framework where AI is deployed by law enforcement, migration, and national security forces.[127]

[120] GDPR, *supra* note 95, at art. 5(1(a).

[121] EU AI Act, *supra* note 11, at art. 49(4).

[122] *See generally* EDRi & AI Coalition Partners, *EU's AI Act fails to set gold standard for human rights*, EDRi (Apr. 3, 2024), https://edri.org/our-work/eu-ai-act-fails-to-set-gold-standard-for-human-rights/.

[123] *See id.*

[124] GDPR, *supra* note 95, art. 5(1)(b).

[125] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 2024/1689) 67.

[126] *A Dangerous Precedent: How the EU AI Act Fails Migrants and People on the Move, Platform, Platform for Int'l. Coop. on Undocumented Migrants*, PICUM (Apr. 4, 2024), https://picum.org/blog/a-dangerous-precedent-how-the-eu-ai-act-fails-migrants-and-people-on-the-move.

[127] *Id.* ("Perhaps the most harmful aspect of the EU AI Act is the creation of a parallel legal framework when AI is deployed by law enforcement, migration and national security authorities. As a result of pressure exerted by Member States, law enforcement and security industry lobbies, these authorities are explicitly exempted from the most important rules and safeguards within

Third, the GDPR provides extra protection for categories of data, including biometric data.[128] In Articles 9(1) and 9(2), these protections are mentioned to be permitted under strict conditions.[129] The AI Act also defines biometric data as a special category in Annex III, including remote biometric identification, AI to be used for biometric categorization, and emotion recognition.[130] It has been shown that this form of data collection has been tested on refugees in Greece and Hungary, while in Germany, dialect recognition programs are used.[131]

Although the AI Act facially aligns with the principles set out in the GDPR, the broad and undefined exemptions in border control risk creating a system that is functionally tiered: one system for EU citizens and a separate system for refugees and migrants. The protections may not apply since the AI Act does not apply to the processing of personal data if it involves "the safeguarding against and the prevention of threats to public security."[132] Border control is within the broad notion of "public security," so emotion recognition is prohibited in the workplace and educational institutions, but not at the borders.[133] Further, AI is prohibited from evaluating individuals based on assumed characteristics but may not be prohibited to do so at the borders,[134] and AI is prohibited in predictive policing for EU citizens, but not at the border.[135] Thus, the effectiveness of the GDPR will depend on how broadly member states will interpret such exemptions which allow for improper collection and use of data.

2. Common European Asylum System

The Common European Asylum System (CEAS) implements standards to ensure that asylum seekers are treated fairly and equally across member states.[136] A cornerstone of the CEAS is the Dublin III

the AI Act."). *See also* Ludivine Sarah Stewart, *The Regulation of AI-Based Migration Technologies Under the EU AI Act: (Still) Operating in the Shadows?*, 30 EUR. L. J. 122, (2024).

[128] GDPR, *supra* note 95, art. 9.

[129] *Id.*

[130] EU AI Act, *supra* note 11, annex III(1).

[131] OZKUL, *supra* note 3, at 5-6; Ben Knight, *Germany to Test Speech Recognition Tech on Refugees*, DW (May 26, 2017), https://www.dw.com/en/germany-failed-to-use-language-recognition-tech-on-refugees/a-39001280.

[132] EU AI Act, *supra* note 11, art. 3(45).

[133] *Id.*, recital 33.

[134] *Id.*, art. XX, annex III. *See also id.*, recitals 29, 30, 60.

[135] *Id.*, art. XX.

[136] *See generally Common European Asylum System*, EUR. COMM'N: MIGRATION & HOME AFFS., https://home-affairs.ec.europa.eu/policies/migration-and-asylum/common-european-asylum-system_en (last visited June 2024).

Regulation, which determines which EU member state is responsible for asylum application examination.[137] In examining asylum rights regarding Dublin III, the ECJ establishes a clear precedent that procedural or technical rules cannot override fundamental rights. In *C.K. and Others v. Republic of Slovenia*, the ECJ found that transfers to other member states *must* be blocked if a real risk of inhumane or degrading treatment exists.[138] There, the Court rejected a mechanical approach that did not consider individual situations, even absent systemic deficiencies.[139] In the context of the AI Act, the idea of individualized assessment is important considering that AI data relies on historical patterns.[140] AI systems rely on historical data shaped by existing power structures on social inequality, the biases are adopted by the generative AI systems.[141] The use of historical patterns may induce discriminatory practices that flag and attack vulnerable populations, leaving them up for transfer by member states exercising their "national security" concerns. In a situation like border control, where human judgment and ethical considerations are critical, the use of generative AI can lead to harmful impacts on migration communities. The harmful impacts can lead to detainment, data collection, visa delays or denials. Again, member states will have broad control as to the extent of discrimination that refugees face at the borders and during processing.

Assuming that this automated decision-making and data capture results in increased harassment against asylum seekers, or increased rejection of applications or transfers, it is important to recognize further safeguards supposedly available. In *Aranyosi and Căldăraru v. Generalstaatsanwaltschaft Bremen*, the Court emphasized that human dignity must be considered even in cases of extradition, where one cannot be surrendered if they would be subject to "inhuman or degrading treatment."[142] The safeguard of "human dignity"' is reduced by the

[137] Regulation 604/2013 Dublin III Regulation, of the European Parliament and of the Council of 26 June 2013, establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast), 2013 O.J. (L 180) recital 1, 31.

[138] *See* Case C-578/16, C.K. v. Republic of Slovenia, ECLI:EU:C:2017:127, ¶ 65 (Feb. 16, 2017).

[139] *See id.* ¶¶ 42-43.

[140] *See* Katharina Mosene, *One step forward, two steps back: Why Artificial Intelligence is currently mainly predicting the past*, HUMBOLDT INST. FOR INTERNET AND SOC'Y. (Oct. 15, 2024), https://www.hiig.de/en/why-ai-is-currently-mainly-predicting-the-past/.

[141] See *id.*

[142] Case C-404/15, Aranyosi and Căldăraru v. Generalstaatsanwaltschaft Bremen, ECLI:EU:C:2016:198, ¶ 91 (Apr. 5, 2016).

AI Act's exemptions, which enable automation in a system where discrimination is already rampant—at EU airports, for instance, many respondents in a study believed that secondary screening occurred because of their race, appearance, or religious beliefs.[143] This higher rate of discrimination occurs in the public context of traveling, where other travelers can observe discrimination takes place. Without any oversight, in a private setting, concerning an already vulnerable population, this Note assumes that AI will only proliferate the already-existing discrimination. The impact of this discrimination may cause increased denial of asylum applications, forcing vulnerable communities to either face illegal status in a safer country or return to an environment where inhuman treatment is more likely to occur.

The Asylum Procedures Directive also places nominal protections as it requires "individual, objective" examination.[144] As stated, the AI Act permits automation and data capture in a system that relies on skewed data without doing individual examination.[145] Studies find that error rates for dark-skinned individuals are significantly higher than light-skinned individuals in biometric identification systems.[146] Similar to other generative AI, biometric identification systems use a database of known identities.[147] The AI Act will create dangerous conditions, seeing that a majority of asylum seekers in the EU have been those from Africa and the Middle East, who typically will have a different complexion not common in biometric galleries.

[143] EUR. UNION AGENCY FOR FUNDAMENTAL RTS. [FRA], DIGNITY: FUNDAMENTAL RIGHTS AT AIRPORTS: BORDER CHECKS AT FIVE INTERNATIONAL AIRPORTS IN THE EUROPEAN UNION 49, 122 (2014) doi:10.2811/68358.

[144] Council Directive 2013/32/EU, of the European Parliament and of the Council of 26 June 2013 on Common Procedures for Granting and Withdrawing International Protection (Asylum Procedures Directive), 2013 O.J, (L 180) art. 10.

[145] *See* Mosene, *supra* note 140.

[146] *See generally* William Thong et al., *Beyond Skin Tone: A Multidimensional Measure of Apparent Skin Color*, arXiv 9 (Oct. 3, 2023) https://arxiv.org/pdf/2309.05148. *See also* CYNTHIA M. COOK ET AL., DEMOGRAPHIC EFFECTS ACROSS 158 FACIAL RECOGNITION SYSTEMS, DEP'T OF HOMELAND SEC. SCI. & TECH. DIRECTORATE 21 (2023) ("For 57% of models, those with darker skin had lower mated similarity scores. We further show that, for models where skin lightness is found to be significant, skin lightness is a better predictor of average mated similarity scores than self-reported race.").

[147] *Id.*; *Ban Dangerous Facial Recognition Technology That Amplifies Racist Policing*, AMNESTY INT'L (Jan. 26, 2021) https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/ (Amnesty International calling for ban on policing that uses AI that may amplify racist policing).

V. Recommendations for EU AI Law Reform

To address these concerning disparities and protect vulnerable migrants, the following recommendations should be implemented into the EU AI Act. Most importantly, there must be a comprehensive ban on biometric surveillance that does not have a clearly defined purpose. Without a clear definition or scope of surveillance, biometric data can be used for vague or unauthorized purposes that contribute to discrimination, and other rights violations, against refugees and asylum seekers. To remedy potential injustices, proactive steps can be taken: the prohibition on real-time and remote biometric identification in public spaces, including detention facilities; the removal of current exemptions for "imminent threats" unless "imminent" is clearly defined; the expansion of the definition of public spaces, where broad surveillance is prohibited, to include border areas; and a ban of biometric systems that enable racial or gender profiling.

Furthermore, the EU must take actions to prohibit predictive and automated AI systems since there exists a history of profiling against protected groups. Several other actions can be taken to correct harmful practices: banning systems that make individual risk assessments based on race, religion, and gender, banning emotion recognition systems that predict mental states in asylum cases, and banning AI systems that rely on historical inputs (inputs that have track records of discrimination against Arab, African, and/or Muslim migrants).

Additional measures can take the form of requiring specific justifications for "security" based exemptions, implementing oversight mechanisms and independent oversight bodies for AI use in migration contexts, and mandating the documentation of data sources and methodologies, the capabilities and limitations of AI used, and regular fundamental rights impact reports.[148]

Some may argue that if these recommendations were to be implemented, member states would be constrained in their ability to protect their borders. To them, the currently broad AI capabilities are necessary to analyze and efficiently identify threats due to the high volume of people crossing into, and through, EU borders.[149] However, there is a

[148] *See* PROTECT NOT SURVEIL, STOPPING THE UNFETTERED EXPANSION OF EUROPOL'S DIGITAL SURVEILLANCE POWERS AGAINST MIGRANTS 3 (February 2025).

[149] Maria Maggiore et al., *France Spearheads Member State Campaign to Dilute European AI Regulation*, INVESTIGATE EUR. (Jan. 22, 2025), https://www.investigate-europe.eu/posts/france-spearheads-member-state-campaign-dilute-european-artificial-intelligence-regulation. ("When ambassadors met in the Coreper on 18 November 2022, France's representative was unequivocal about the country's wishes, according to the meeting minutes obtained. "The exclusion of security and

flaw in this argument; security and rights protection are not mutually exclusive. According to *Johnston,* to use a national security exemption, the measures must be proportionate and non-discriminatory.[150] The current exemptions are neither proportionate nor non-discriminatory: there is no systematic link between increased national security threats and refugee populations. Using predictive AI, with error rates for certain demographics, will worsen unequal treatment of minority and vulnerable communities.[151]

With these counterarguments in mind, if the EU were to implement these changes into an amended AI Act, it would close the gaps in fundamental rights protections that exist due to the "security" exemptions. The recommendations put forth also better align with existing jurisprudence. For instance, banning biometric surveillance without a defined purpose would uphold the "strictly necessary" and proportionate provisions in *Digital Rights Ireland*, meant to protect one's Article 7 right to privacy.[152] Similarly, banning the use of predictive AI systems, which have been shown to rely on discriminatory information, would support one's right to not be discriminated against under Article 21 of the CFREU.[153] Lastly, the oversight mechanisms proposed would go to strengthen the data protection one has under Article 8, preventing indiscriminate data retention, without strict purpose, that was prohibited in *La Quadrature du Net*.[154]

These changes will require amendments to the EU AI Act that include adequate resources and the development of new oversight bodies. It is the hope that once these recommendations are implemented, the AI Act

defence . . . must be maintained at all costs." It was a reference to a part of the law proposing that only the military would be allowed to conduct surveillance in public spaces. France wanted an exemption for all authorities if necessary for 'national security.' At a later meeting Italy, Hungary, Romania, Sweden, the Czech Republic, Lithuania, Finland and Bulgaria all expressed support for the French position.")

[150] Case C-222/84, Johnston v. Chief Constable of the Royal Ulster Constabulary, ECLI:EU:C:1986:206, ¶¶ 17, 38-39 (May 15, 1986).

[151] *See* Nada Hassanin, *Law Professor Explores Racial Bias Implications in Facial Recognition Technology*, U. CALGARY NEWS, (Aug. 23, 2023), https://ucalgary.ca/news/law-professor-explores-racial-bias-implications-facial-recognition-technology (discussing how biased training data can lead to biased results).

[152] Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, ECLI:EU:C:2014:238, ¶¶ 52-53 (Apr. 8, 2014).

[153] CFREU, *supra* note 19, art. 21.

[154] Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net v. Premier ministre, ECLI:EU:C:2020:6, ¶ 164 (Oct. 6, 2020) ("To the extent that the purpose of such expedited retention no longer corresponds to the purpose for which that data was initially collected and retained and since any processing of data must, under Article 8(2) of the Charter, be consistent with specified purposes").

will better comply with existing ECJ jurisprudence and prevent AI from overriding fundamental rights for those seeking safe harbor in the EU.

VI. Conclusion

The EU AI Act, while the first comprehensive attempt to regulate and standardize AI use across the EU, implements exemptions in border control and policing that contradict the EU's Charter of Fundamental Rights. The broad claims of "security" create substantial risks for refugees and asylum seekers. Furthermore, the way the AI Act has been currently written will lead to a tiered system where EU nationals are entitled to increased protections while already vulnerable populations suffer a system that diminishes their rights.

The analysis presented examines how the AI Act is currently inconsistent with established EU jurisprudence regarding privacy, data protection, asylum rights, and non-discrimination. Case precedent was used to show a clear understanding that the facially "neutral" policies in the AI Act cannot be allowed to enable discriminatory practices. The current EU border practices build on frameworks that have allowed for significant discrimination against African, Arab, and Muslim populations, with documented patterns of systematic bias. If the EU AI Act does not clearly define how its system relies on historical practices, and how it is currently employed, the exemptions will only serve to amplify the fundamental rights violations. The technology used, from emotion recognition and biometrics to predictive policing, sets a dangerous standard for how AI can be used to attack those seeking refuge in the EU.

To address the rights violations, substantial reforms are needed that will more clearly define "security" and implement independent oversight mechanisms. Explicit protections for refugees must be included. Without reform, the EU AI Act will not live to be the rights-protective framework it claims to be. The EU must reconcile its interest in innovation with its obligation to protect society's most vulnerable–refugees, migrants, and marginalized communities whose futures hang in the balance of algorithmic decision-making.