Legal and human rights implications for AI: challenges and liabilities

Pranay Meshram[1], Priya Meshram[2]

KIET Group of Institutions, Delhi-NCR, Ghaziabad, UP, India [1], Yeshwantrao Chavan , College of Engineering, Nagpur, India [2]
pranay.meshram@kiet.edu [1], priyameshram1485@gmail.com [2]

Abstract:
Here we talks about the problems and legal rights related to artificial intelligence (AI). It discusses how people are talking about these issues and what problems still need to be solved. Some of the problems are: AI being secretive, being not safe from hackers, being unfair, causing bias and discrimination, having no clear rules, and causing problems with ownership and privacy. It also talks about who is responsible when AI causes harm. The concept of "vulnerability" is used throughout the essay to grasp the major issues and how to make things better for individuals. It acknowledges the good work being done in AI law but says that we still need to keep improving because AI has big impacts, especially on people who are already in a tough spot, and on their rights.
Keywords : **artificial intelligence, cybersecurity, data protection, legal rights, vulnerability**

Introduction :

According to Boden (2016), Artificial Intelligence (AI) is widespread in today's society, and its rapid progress in development, deployment, and use significantly contributes to the worldwide economy. (McKinsey 2019; PwC 2017). While AI has tremendous advantages, such as improvements in creativity, services, safety, and problem-solving, it also raises concerns about its potential negative impacts on human autonomy, privacy, and fundamental rights and freedoms, as emphasized by the OECD in 2019. The legal discussion on the legal and human rights aspects of AI is well-established, with detailed analyses of specific issues found in Sections 3 and 4 of this article. However, the regulatory landscape is dynamic, requiring an exploration of a comprehensive range of issues. A thorough analysis and mapping of sensitivity to these concerns are notably lacking. The main research questions addressed here include identifying the legal and human rights issues related to AI, examining current approaches to address them, identifying gaps and challenges, and proposing strategies to reduce vulnerability and enhance flexibility in this context.

This article is structured with an initial overview of legal and human rights issues in Section 3, followed by an in-depth examination of specific legal concerns related to AI in Section 4. In Section 5, the focus shifts to proposed solutions, their implementation, existing gaps and challenges, and their impact on human rights principles. The article links legal issues to prominent international human rights treaties, offering examples of corresponding human rights principles at both global and regional levels. Section 6 adopts the perspective of 'vulnerability' to comprehensively analyze identified critical areas of concern, providing guidance for efforts to mitigate AI risks and impacts to safeguard human and societal well-being. Recognizing existing contributions in the AI law domain, as evident in the cited

literature, this associated analysis aims to offer additional perceptions and stimulate ongoing considerations on this vital issue. Given the widespread use of AI and its substantial influence on persons and their human rights, the article underscores the importance of continued dialogue and exploration in this field.
Section 4 provides a broad summary but does not encompass all the legal complexities and human rights challenges associated with AI.

To determine legal issues and challenges associated with AI, the search included relevant literature from genuine academic journals. and professional journals, books, as well as previous policy research. Keyword s like 'legal/human rights issues + AI/artificial intelligence/machine learning' were employed over a span of five to ten years. Supplementary sources such as SSRN and Google Scholar were consulted to identify high-impact issues. Selected references underwent further scrutiny to uncover potential unknown issues. The issues chosen were influenced by their coverage in current legal and policy literature, as well as their impact on society values and lifestyles, and their controversial nature. However, this study has limitations in terms of its temporal and language scope, concentrating on English-language research during a specific period. A comprehensive analysis, usually conducted by other scholars, is beyond the study's scope, as each issue merits individual, in-depth exploration, considering the specific applicable legal provisions.

To align legal concerns with the principles outlined in international human rights treaties like the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social, and Cultural Rights (ICESCR), the Universal Declaration of Human Rights (UDHR), the United Nations Charter, the Convention on the Prohibition or Bans on certain Conventional Weapons that may be considered to have excessively harmful or desultory effects, and the convention on the prohibition or restrictions reviewed.

The approach of examining AI legal issues in the context of real-world situations was employed to link these issues to the populations most at risk and the factors influencing their vulnerability. The identification of vulnerable groups and determining variables was based on a comprehensive study of literature, supplemented by online searches to uncover additional cases. It's important to note that the resulting table is not exhaustive and may undergo changes when scrutinized in different settings.

Legal and human rights issues of AI:

This section discusses various legal and human rights challenges in relation to artificial intelligence (AI) are examined. The analysis explores the significance of each issue, potential remedies or ongoing efforts to address them, and the associated gaps and obstacles. While acknowledging that extensive research has individually scrutinized each topic, the aim here is to provide an updated and comprehensive overview for future research purposes. The presented concerns encompass both the design and nature of AI, as well as the challenges tied to its implementation and application, often interlinked. Certain challenges have broad consequences across different domains, affecting numerous industries or fields of application. Some issues, like privacy/data protection, are overarching concerns for all technologies, while others, such as transparency, fairness, and accountability, are interdependent

and not isolated. It is underscored that the potential for AI to amplify negative consequences should not be underestimated.

A specific concern brought to attention is the absence of algorithmic transparency, considered noteworthy in legal conversations about AI. The lack of transparency gives rise to apprehensions, especially in high-risk domains, prompting demands for AI to uphold accountability, fairness, and transparency. Examples of individuals being adversely affected by undisclosed algorithmic decisions are cited. Numerous proposals have been made, including activities such as raising awareness, establishing accountability in public-sector algorithm usage, regulatory supervision, legal responsibility, and universal collaboration for algorithm governance. Precise strategies advocated to improve algorithmic transparency include completing algorithmic effect assessments, defining a transparency standard for self-governing systems, offering counterfactual explanations, and implementing local interpretable model-agnostic explanations. However, it is noted that transparency has limitations, and some proposed solutions, such as algorithmic impact assessments, are still in the early stages of development and require further evaluation. This underscores the need for future research and assessment in this area.

Cybersecurity Vulnerabilities:

Issues:

A RAND perspectives paper by Osoba and Welser (2017) highlights the problem of cybersecurity vulnerabilities, revealing a range of security issues associated with AI. These worries include the risk of errors and fatalities as a because of totally automated decision-making, the employment of AI weaponry without human participation, and AI cybersecurity vulnerabilities. The use of AI in national security, particularly in surveillance and cybersecurity, poses a new risk known as the 'data diet issue.' AI deployed overseas via network intervention methods poses larger and more strategic threats, such as sophisticated social media targeting of political messaging. Domestic security risks are also highlighted in the study, such as governments increasingly employing artificial agents for civilian monitoring, raising worries about potential infringement of fundamental citizens' rights (Couchman, 2019). These challenges are important because they expose vital arrangements to possible damages, which can have serious consequences for society and people, posing hazards to life, human security, and resource access. The concealed nature of cybersecurity vulnerabilities poses an additional threat, often revealed only after damage has occurred.

Proposed Solution:

To address these challenges, various solutions and technologies have been developed or applied. These encompass implementing robust protection and recovery mechanisms, tackling vulnerabilities during the design stage, involving human analysts in crucial decision-making, adopting risk management programs, and conducting software upgrades (Fralick, 2019). Yet, effectively addressing these issues requires the practical and responsive application of cybersecurity policies, mechanisms, and tools at every phase of AI development, spanning from design and implementation to utilization. Despite the existence of solutions, putting them into practice remains a challenge, as underscored in a SHERPA

report. The paper emphasises the importance of deliberate thinking in machine learning system architecture decisions in order to defend against potential attacks and make well-reasoned trade-off judgements regarding model complexity, explainability, and resilience (Patel et al., 2019).

Unfairness, Bias, and Discrimination:

Issues:

In the usage of algorithms and automated decision-making systems, unfairness, prejudice, and discrimination appear as recurring concerns, affecting numerous sectors such as health, work, credit, criminal justice, and education. Notable instances, like the controversial exams algorithm used in England in 2020, have led to protests and legal challenges (Ferguson & Savage, 2020). The EU Agency for Fundamental Rights (FRA) underscores the latent for algorithmic discrimination against individuals, highlighting the importance of taking into account the principle of non-discrimination in the application of algorithms in daily life (FRA, 2018). The European Parliament stresses the potential for unequal treatment and indirect discrimination, particularly in the domains of education and employment (European Parliament, 2017).

Solutions:

Numerous proposals aim to address these issues, including regular assessments of data set representativeness, Incorporating humans in decision-making processes and establishing certification procedures to ensure that algorithmic decision systems steer clear of unjustified bias are crucial. The IEEE P7003 Standard for Algorithmic Bias Considerations and open-source toolkits like AI Fairness 360 offer frameworks and metrics for assessing, reporting, and mitigating discrimination and bias in machine learning models (European Parliament, 2017). However, challenges persist, including gaps in legal protection against discriminatory behavior, tensions in implementing humans-in-the-loop approaches, concerns about the understandability and discoverability of private data, and the need for a comprehensive and an ethical approach to algorithmic audits (Guszca et al., 2018; House of Commons, 2018; Raji & Buolamwini, 2019).

Lack of Contestability:

Issue:

The right of individuals to contest automated decisions significantly affecting their rights or legitimate interests is a crucial aspect of data protection law. Yet, as outlined by Hildebrandt (2016), the lack of transparency in machine learning (ML) systems diminishes the accountability of their owners and limits the ability to challenge their decisions. Edwards and Veale (2017) point out that algorithmic systems lack contestability because there are no evident means to question them when they yield unexpected, harmful, unfair, or discriminatory outcomes. Bayamlıoğlu (2018) underscores the imperative nature of an acceptable level of contestability in protecting individual dignity and basic rights. Contestability, viewed as an essential aspect of the rule of law, as well as democratic government, is associated with the 'human element' of judgment.

Proposed Solution:

Proposed solutions include making contestability a prerequisite at every phase of an artificial intelligence system's lifetime (Almada, 2019). However, Roig (2017) suggests that generic protections may be insufficiently effective in the context of automated processing based on data analysis, creating

difficulties in opposing choices that lack clear reasons. To resolve this issue, extensive efforts are required at the design, development, and utilisation stages.

Legal Personhood Issues:

The ongoing debate revolves around whether existing legal categories can put up AI or if a new category should be established. The European Parliament (2017) raises the question of whether AI systems could be regarded as legal subjects, presenting both a legal and politically profound problem. The High-Level Expert Group on Artificial Intelligence (AI HLEG) strongly objects to the idea of AI systems obtaining legal personhood. citing inconsistencies with human agency, accountability, and responsibility. Despite debates suggesting potential justifications for legal personality for AI, caution prevails in the EU against establishing a novel legal identity for AI systems. (Siemaszko et al., 2020; Bryson et al., 2017).

Solutions concerns about legal personhood for AI on an international, EU, or national scale have not seen significant breakthroughs, with difficulties arising from the political sensitivity of the matter.

Intellectual Property Issues:

Intellectual property rights, considered to have a human rights character, are implicated in various policy areas, raising questions about the ownership of AI-generated works, patentability of AI inventions, and the ownership of datasets used for AI learning. Rodrigues (2019) notes that laws may offer diverse solutions to these issues, with the UK, for instance, protecting computer-generated works and addressing ownership based on employment or commission. However, many intellectual property issues related to AI remain unresolved, especially as AI advancements complicate the identification of creators, demanding further research and exploration (Davies, 2011; Talking Tech, 2017).

Privacy and Data Protection Issues:

The Importance of the Problem:

Legal scholars as well as data protection authorities, such as CNIL and ICO, argue that AI poses significant challenges to privacy and data protection (CNIL 2017; ICO 2017). These challenges encompass issues like informed consent, surveillance, breach of data protection rights, and the possibility of increased privacy concerns and surveillance capabilities (Gardner 2016; Brundage 2018; EDPS 2016; ICO 2017).

Proposed Solutions and Addressing the Issues:

Privacy and data protection laws, predominantly within the EU, are deemed to provide good safeguards against infringements of data subjects' rights. GDPR rights such as transparency, access to information, correction, deletion, and the right to object to automated decision-making are identified as critical protections (GDPR; Rigby 2019). Transparency regarding possible hazards is emphasised in the usage of AI., and developers are urged should be mindful of ethical and regulatory constraints in data processing. Privacy measures like anonymization, confidentiality notices, impact assessments, privacy by design, ethical principles, and auditable machine algorithms are proposed to address privacy and data protection concerns (Vayena, Blasimme & Cohen 2018; Brundage 2018; ICO 2017).

Identified Gaps and Challenges:

Privacy and data protection regulations provide safeguards., they do not cover all AI-related issues comprehensively. Challenges include the evolving nature of AI and the difficulty of aligning data protection laws with rapidly changing AI contexts. The efficiency of privacy and data protection measures relies on their accurate application, monitoring, and enforcement. Furthermore, the noted challenge includes the constrained adoption of privacy by design and default in commercial products and services (CIPL 2018).
Liability for Damage:

The Significance of the Issue:

The utilization of AI technologies may lead to damage to individuals and property, such as accidents involving driverless cars, drone crashes, or wrongful medical diagnoses by AI software (Gluyas and Day 2018).

Proposed Solutions and Addressing the Issues:

Addressing liability issues related to AI involves considering civil and criminal liability, product design legislation, and consumer protection laws. Discussions discover whether criminal liability can apply to AI entities and propose supplementary rules to establish legal frameworks suitable for robots based on AI. Suggestions include monitoring duties, included emergency brakes, continual assistance, and patching tasks. to establish presumed negligence and liability (Kingston 2016; Hallevy 2015; Rachum-Twaig 2020).

Identified Gaps and Challenges:

Strict liability is considered inadequate due to the unpredictable nature of AI, and adjustments to existing liability regimes are recommended to account for the complexity, modification, and vulnerability of emergent digital technologies (Bathee 2018).

Inadequate Accountability for Harms:
The Impact of the Issue:

Accountability in AI system development, deployment, and application is crucial for hazard organization and addressing the "accountability gap." Challenges arise in interconnection, justice, and compensation when harm occurs due to AI (AI HLEG 2020; Bartlett 2019; Privacy International and Article 19 2018).

Proposed Solutions and Addressing the Issues:

Legal accountability mechanisms, such as the "right to explanation," data protection, transparency safeguards, auditing, and reporting obligations, are suggested to address accountability gaps (Wachter, Mittelstadt, and Floridi 2017; Edwards, Veale 2017; Doshi-Velez et al 2017).

Identified Gaps and Challenges:

Challenges include the imperfect nature of AI accountability solutions, potential chilling effects on AI development when holding developers responsible, and the practical difficulty of explaining all algorithmic decisions (Bartlett 2019; Wallace 2017; Edwards & Veale 2017).

Affecting Human Rights Principles:
Treaties addressing international human rights, while not explicitly mentioning AI, cover a broad spectrum of rights principles that are affected by AI developments. Privacy, data protection, non-discrimination, equality, and access to justice are prominently discussed, with other principles requiring more attention and research (Andorno 2016).

Issues and Vulnerability:

Vulnerability is recognized as a critical aspect in understanding the impact of AI on individuals and communities. Vulnerability varies across physical/technical, social, political, regulatory, and economic dimensions. Vulnerable groups, such as those with limited resources, increased morbidity risks, women-headed households, ethnic minorities, and disabled individuals, are particularly susceptible to harm from AI applications (EquiFrame conceptualization; Andorno 2016).

AI Issue	Who find the issue (Researcher)	Human rights principles that might be affected	Solutions
Lack of algorithmic Transperaency	Bodo et al 2018; Coglianese & Lehr 2018; Lepri Pasquale 2015 Cath 2018	A just trial and proper legal procedures, efficient solutions, social entitlements and availability to public services, and the entitlement to engage in elections at no expense.	1.awareness raising 2. Responsibility in employing algorithmic decision-making within the public sector, 3. Legal liability and regulatory examination, 4. International cooperation in the

			governance of algorithms..
Cybersecurity vulnerabilities	Osoba and Welser (2017)	The entitlement to personal privacy, the liberty to express oneself, and the unrestricted movement of information	Different approaches and instruments are currently in use.
Unfairness, bias and discrimination	Unfairness (Smith 2017), bias (Courtland 2018) and discrimination (Smith 2017)	The eradication of any type of bias against women; parity in rights for both males and females have equal access to children's rights without discrimination, and there is fairness before the law with impartial protection under legal provisions.	IEEE offers People or entities developing algorithmic systems can employ this method to prevent undesired, unjustifiable, and unreasonably unequal outcomes for users.
Lack of contestability	Edwards and Veale (2017 Bayamlıoğlu (2018)	Entitlement to a meaningful remedy and the ability to access justice.	safeguarding of rights in decisions solely reliant on automated processing. This involves making it a necessary requirement at every phase of an artificial intelligence system's lifecycle.
Legal personhood	Burri (2017). Čerka et al (2017) (AI HLEG 2019).	The entitlement to be acknowledged as a person under the law universally, the right to equal treatment, and the elimination of all types of discrimination.	There hasn't been a notable advancement in resolving legal personhood concerns for AI on the global, EU, or national scale. Although this matter has been brought up, there's yet to be an

			international or even regional consensus.
Intellectual property issues	The International Covenant on Eco-nomic, Social and Cultural Rights (ICESCR, Article 15), the International Covenant on Civil and Political Rights (ICCPR, Article 19) and the Vi-enna Declaration and Programme of Action (VDPA) 1993.	The entitlement to possess property individually or in collaboration with others; the freedom to actively engage in the social activities of the public, relish the arts, and partake in scientific progress and its advantages; and the right to safeguard the ethical and physical interests arising from any scientific, literary, or artistic creation for which one is the creator.	Legal provisions safeguard works of literature, drama, music, or art that are generated by computers.
Adverse effects on workers	The IBA Global Employment Institute report (2017)	Entitlement to social security, prevention of discrimination in the exercise of the right to work, freedom to choose employment, fair and favorable working conditions, protection against unemployment, equal pay for equal work, and fair and favorable compensation.	These include retraining workers and refocusing and adjusting the education system (UK House of Lords 2018). As per the European Commission's Communication on Artificial Intelligence for Europe (2018), it is recommended that governments give priority to updating education at various levels, ensuring that everyone has ample opportunities to acquire the necessary skills.

Issues and vulnerability

Addressing legal concerns, gaps, and obstacles related to AI is not enough. Examining these issues through the concept of 'vulnerability' will greatly assist in consolidating key areas of concern and guide efforts to mitigate the risks and impacts of AI, ensuring the better preservation of human and societal well-being. This approach will also ensure that AI technologies enhance human rights for all, with a particular focus on the most vulnerable individuals.

Definitions of vulnerability are scattered, encompassing the general idea of being exposed to the potential for harm, whether physically or emotionally, as indicated by Lexico. It can also denote a susceptibility that may be exploited by one or more threats or a predisposition to suffer damage. Another perspective defines vulnerability as the diminished capacity of an individual or group to anticipate, cope with, resist, and recover from impacts, according to the International Federation of Red Cross and Red Crescent Societies. Vulnerability is not static; it changes over time in terms of characteristics, driving forces, and levels, as noted by Vogel & O'Brien (2004) and DFID (2004). It stands in contrast to 'resilience,' which refers to the ability of individuals, households, communities, countries, or regions to withstand, adapt to, and rapidly recover from stressors and shocks, as outlined by the European Commission in 2012. Scholarly and policy discussions categorize various vulnerable groups, with EquiFrame conceptualizing 12 categories, such as those with 1. limited resources . 2. Heightened relative risk for illness (pertaining to individuals with one of the top 10 diseases identified by the WHO within the relevant country). 3. Maternal-child mortality pertains to factors affecting the health of both mothers and children in the age group of 0–5 years. 4. Female-headed families (denoting households led by a woman). 5. Special needs kids (indicating children marginalized by specific circumstances, such as orphans or street children). 6. Elderly individuals (referring to those in older age). 7. Adolescence (pertaining to younger age without specifying gender). 8. Minorities of ethnic origin (representing non-majority groups concerning culture, race, or ethnic identity). 9. People who have been displaced (relating to individuals who, due to civil unrest or unsustainable livelihoods, have been forced from their previous residences). 10. Dwellers located far from services (indicating individuals living a considerable distance or time away from health services). 11. Individuals with chronic illnesses (referring to those with conditions requiring ongoing care). 12. People with disabilities.

To be more specific, as outlined by Andorno (2016), in the context of human rights discussions, the term "vulnerability" denotes an increased susceptibility of specific individuals or groups to potential harm or injustice inflicted by others or the state. Among those more prone to harm, exploitation, or discrimination are children, women, older individuals, people with disabilities, and members of ethnic or religious minority groups. Andorno emphasizes that characterizing these groups as 'vulnerable' doesn't imply their elevation above others; rather, it reflects the harsh reality that these groups are more likely to face discrimination or other human rights violations. This relevance to our discussion is significant, as all these categories are implicated in legal issues and human rights principles at stake in some form or manner.

The implementation and utilization of AI technologies have a disproportionate impact on vulnerable groups. For instance, the UNESCO COMEST Preliminary Study on the Ethics of Artificial Intelligence

cites the Allegheny Family Screening Tool (AFST) as an example, a predictive model designed to forecast child neglect and abuse. The study highlights that this tool "exacerbates existing structural discrimination against the poor and has a disproportionately adverse impact on vulnerable communities" by over presenting the poor and utilizing proxies that inherently disadvantage economically disadvantaged working households. Beduschi (2020) expresses concerns about the increasing reliance on technology to collect personal data from vulnerable groups, for instance, individuals like migrants and refugees may face extra administrative obstacles that could lead to their exclusion from receiving protection.
Children, as noted by Butterfield-Firth (2018) and the ICO, are particularly vulnerable in the AI context. The ICO explains that children may have difficulty understanding how their data is used, anticipating its effects, and protecting themselves from unfavorable repercussions. Additionally, individuals from the LGBTIQ community might experience adverse effects from systems that allow or encourage profiling or prejudice.

Furthermore, because of their significant use of AI and big data, AI-powered, data-driven economies may be more attractive prospects for cyberattacks. In the AI context, vulnerability is influenced by various factors such as...

In the AI context, vulnerability is influenced by several factors, and these can vary across different scenarios and applications. Some key factors include:

Access to Technology: Disparities in access to AI technologies can contribute to vulnerability. Individuals or groups with limited access to AI tools and resources may face challenges in benefiting from or defending against the impacts of AI.

Data Quality and Bias: The quality and bias present in training data used to develop AI systems can significantly impact vulnerability. If training data is incomplete, biased, or unrepresentative, the AI system may produce discriminatory or unfair outcomes, disproportionately affecting certain groups.

Transparency and Explainability: Lack of transparency and explainability in AI systems can contribute to vulnerability. If individuals, especially those from marginalized communities, cannot understand how AI decisions are made, they may be more susceptible to unjust or harmful consequences.

Legal and Ethical Safeguards: The absence of clear legal frameworks and ethical safeguards for AI applications can render individuals and communities more vulnerable. Inadequate regulations may fail to protect against misuse, discrimination, or other negative impacts of AI technologies.

Education and Awareness: Levels of education and awareness about AI and its implications can influence vulnerability. Those with limited understanding of AI may be less equipped to navigate its effects, protect their rights, or advocate for fair and ethical AI practices.

Socioeconomic Factors: Socioeconomic status plays a crucial role in vulnerability to AI impacts. Economic disparities may result in differential access to AI benefits, exacerbating existing social inequalities.

Intersectionality: Vulnerability in the AI context often involves intersecting factors, such as race, gender, age, and socioeconomic status. The cumulative impact of these factors can create unique challenges and risks for individuals facing multiple forms of discrimination.

Speaking these factors necessitates a thorough strategy that includes policymakers, technologists, and communities in order to assurance that AI technologies are developed, deployed, and regulated in a way that fosters equity, transparency, and inclusion.

Conclusion:

The paper examines the legal difficulties in great detail, gaps, and challenges associated with AI, particularly emphasizing their interconnectedness with human rights principles, It underscores the need for a multi-stakeholder approach, policy and legal adjustments, and technical considerations to address the evolving landscape of AI and its impact on vulnerable groups. The recognized actions involve reducing adverse impacts, building resilience, and addressing root causes to confirm the responsible improvement and deployment of AI technologies. Ongoing monitoring and research are essential to navigate the legal complexities and societal implications as AI technologies continue to advance.

References

1. Access Now (2018) Human rights in the age of artificial intelligence. https://www. accessnow.org/cms/assets/uploads/2018/11/AI- and- Human- Rights.pdf.
2. Almada, M (2019). Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems. In *17th International Conference on Artificial Intelli- gence and Law (ICAIL 2019)* . https://doi.org/10.2139/ssrn.3264189 .
3. . Ananny, M, & Crawford, K (2018). Seeing without knowing: Limitations of the trans- parency ideal and its application to algorithmic accountability. *New Media & Society*, *20* (3), 973–989.
4. Bartlett, M (2019). Solving the AI accountability gap. Hold developers re- sponsible for their creations. *Medium*
5. Beduschi, A (2020). International migration management in the age of artificial intelli- gence. *Migration Studies* , mnaa003.
6. Berk, RA (2019). Accuracy and fairness for juvenile justice risk assessments. *Journal of Empirical Legal Studies* .
7. Brundage M (2018) The malicious use of artificial intelligence: forecasting, pre- vention, and mitigation.
8. Burri, T (2017). International law and artificial intelligence. *German Yearbook of International Law, 60* , 91–108. https://doi.org/10.2139/ssrn.3060191 .
9. Butterfield-Firth, K (2018). Generation AI: What happens when your child's friend is an AI toy that talks back? *World Eco- nomic Forum* .

10. Cath, C (2018). Governing artificial intelligence: Ethical, legal and technical opportu- nities and challenges. *Philosophical Transactions of the Royal Society A: Mathemati- cal, Physical and Engineering Sciences* .
11. CNIL (2017) How Can Humans keep the upper hand? The ethical matters raised by algo- rithms and artificial intelligence. Report on the public debate led by the French Data Protection Authority (CNIL) as part of the ethical discussion assignment set by the digital republic bill.
12. . Coldewey, D (2018). AI desperately needs regulation and public account- ability, experts say. *Techcrunch* .
13. Couchman, H (2019). Policing by machine. *Predictive Policing and the threats to our rights.* . https://www.libertyhumanrights.org.uk/sites/default/files/LIB%2011