United Nations A/79/296

General Assembly

Distr.: General
7 August 2024

Original: English

Seventy-ninth session
Item 71 (b) of the provisional agenda*
Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Human rights in the administration of justice

Report of the Secretary-General

Summary

The present report, submitted pursuant to General Assembly resolution 77/219, serves to highlight the human rights challenges and good practices of the application of digital technologies and artificial intelligence in the administration of justice. It provides a summary of United Nations activities to support States and civil society in their efforts to develop and implement digital and artificial intelligence systems in the administration of justice with a focus on human rights.

* A/79/150.

24-14350 (E) 220824

Please recycle

I. Introduction

1. The present report is submitted pursuant to General Assembly resolution 77/219, in which the Assembly requested the Secretary-General to submit to it at its seventy-ninth session a report on the latest developments, challenges and good practices in human rights in the administration of justice, including on the application of digital technologies in the administration of justice, and on the activities undertaken by the United Nations system. The report draws upon information received from Member States, United Nations entities, human rights mechanisms and civil society, as well as external research.[1]

2. Digital technologies have the potential to contribute to improving access to justice; however, if not developed and used in a human rights-compliant manner, such technologies can exacerbate inequality and discrimination, disproportionately affect marginalized individuals and groups and could potentially affect rights associated with the administration of justice, notably the rights to liberty and security, to a fair trial and to freedom from torture and ill-treatment.[2]

3. The Secretary-General, United Nations entities, experts and the international community recognize that the development, deployment and use of digital technologies and artificial intelligence (AI)[3] should be anchored in human rights.[4] One of the objectives of the global digital compact, as proposed by the Secretary-General, is to "make human rights the foundation of an open, safe and secure digital future, with human dignity at its core".[5] Furthermore, the Secretary-General has indicated that "the use of technology by Member States must also be consistent with international human rights standards".[6]

II. Legal framework and State obligations

4. The human rights norms related to the administration of justice are set out in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. The Covenant recognizes the rights to non-discrimination (art. 2, para. 1); an effective remedy (art. 2, para. 3); life (art. 6); freedom from torture and ill-treatment (art. 7); liberty and security (art. 9); and equality before courts and tribunals and a fair trial (art. 14). Other related rights that may be affected by the use of digital technologies and AI in the administration of justice are the rights to privacy (art. 17);[7] freedom of expression (art. 19);[8] peaceful assembly (art. 21);[9] and freedom

[1] All submissions received from Member States, United Nations entities, human rights mechanisms and civil society organizations cited in the present report can be found at www.ohchr.org/en/calls-for-input/2024/call-input-application-digital-technologies-administration-justice-report.

[2] A/78/184; A/HRC/44/24; A/HRC/48/31; A/HRC/51/17.

[3] There is no internationally agreed definition of AI. The High-level Advisory Body on Artificial Intelligence uses the definition developed by the Organization for Economic Co-operation and Development (OECD). See Stuart Russell, Karine Perset and Marko Grobelnik, "Updates to the OECD's definition of an AI system explained", OECD, 29 November 2023. See also A/73/348.

[4] The life cycle of digital and emerging technologies includes the pre-design, design, development, evaluation, testing, deployment, use, sale, procurement, operation and decommissioning stages, with effective human oversight. See General Assembly resolution 78/265 and the report by the High-level Advisory Body entitled "Governing AI for humanity".

[5] A/77/CRP.1/Add.4, para. 44.

[6] "New vision of the Secretary-General for the rule of law", 31 July 2023.

[7] A/HRC/48/31.

[8] A/73/348.

[9] A/HRC/44/24; Office of the United Nations High Commissioner for Human Rights (OHCHR), "Practical toolkit for law enforcement officials to promote and protect human rights in the context of peaceful protests", 7 March 2024.

of association (art. 22). Other relevant human rights treaties include the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, the International Convention on the Elimination of All Forms of Racial Discrimination, the Convention on the Rights of the Child, the Convention on the Elimination of All Forms of Discrimination against Women and the Convention on the Rights of Persons with Disabilities.

5. The United Nations High Commissioner for Human Rights and the General Assembly are of the view that all technologies must be designed, developed, deployed and regulated in a manner consistent with the relevant obligations of States under international human rights law and the responsibilities of business enterprises to respect human rights.[10] States are required to put into place a framework that prevents human rights violations, holds those responsible to account and provides remedies, in relation to both actions and omissions by the State.[11] Under the principle of due diligence, the State is also required to protect individuals from harm by third parties, including business enterprises. Business enterprises also have responsibilities to respect human rights that should guide their design, development and deployment of technologies.[12] The Guiding Principles on Business and Human Rights provide a "global standard of expected conduct for all business enterprises wherever they operate".[13]

III. AI systems and digital technologies in the administration of justice

6. The present section is focused on AI systems, highlighting several types of digital technologies used in the administration of justice, including applications of such technologies in prisons, court administration, online hearings and electronic monitoring, as well as neurotechnology applications. It contains an analysis of the impact of those systems and technologies on specific human rights.

7. A focus on AI systems is important, as such systems are a component of many digital technologies. From a human rights perspective, common challenges of using AI systems relate to how they are developed, how they operate, how they are monitored and whether sufficient safeguards and oversight are in place.[14] There is uncertainty about the outputs of AI algorithms due to their probabilistic elements and about the human rights impact of the algorithms.[15] AI algorithms are not capable of producing sure predictions; rather, they produce extrapolations based on past data sets.[16] The decision-making processes of many AI systems remain opaque, which means that such systems are "black boxes" that are read and interpreted by complex algorithms. AI systems are still unable to provide a transparent explanation of the reasoning behind the predictions and recommendations being made.[17] In addition, the technology behind the algorithms used in proprietary models is often shielded from

[10] General Assembly resolutions 78/213 and 77/211; OHCHR, "Artificial intelligence must be grounded in human rights, says High Commissioner", 12 July 2023.
[11] CCPR/C/21/Rev.1/Add.13.
[12] A/HRC/38/35.
[13] OHCHR, "Guiding principles on business and human rights: Implementing the United Nations 'Protect, respect and remedy' framework", 2011.
[14] United Nations Interregional Crime and Justice Research Institute (UNICRI) and International Criminal Police Organization (INTERPOL), "Toolkit for responsible AI innovation in law enforcement".
[15] European Union Agency for Fundamental Rights, "#BigData: discrimination in data-supported decision-making", 29 May 2018.
[16] UNICRI and INTERPOL, "Toolkit for responsible AI innovation in law enforcement".
[17] Submission from the Canadian Human Rights Commission.

outside scrutiny, through misuse of intellectual property safeguards.[18] As a result of the very nature of how AI systems function, coupled with a lack of disclosure of data, it can be challenging to meaningfully scrutinize AI-driven recommendations, which can be an obstacle for effective accountability when AI systems cause harm to individuals' rights,[19] and even more so in areas that typically suffer from a general lack of transparency, such as counter-terrorism activities.[20] Courts have found that the use of algorithms has resulted in violations of the right to non-discrimination[21] and that a failure to release the underlying data behind an algorithm constitutes a violation of due process rights.[22] As highlighted by the Secretary-General, additional efforts are necessary to create tools and methods that provide a sufficient level of explanation of how decisions have been reached, in particular when AI is determining critical issues within judicial processes.[23]

A. AI in the administration of justice

8. AI systems increasingly affect all aspects of life, and the administration of justice is no exception. States are increasingly integrating AI systems into law enforcement, national security, criminal justice and border management systems.[24] AI systems are often used as forecasting tools, analysing large quantities of data, including historical data, to assess risks and predict future trends.[25] Predictive policing tools, which may be AI-enabled, make assessments about who might commit future crimes, who might be a victim of those crimes and where those crimes might occur. The use of such tools can trigger interventions by State authorities, such as searches, questioning, arrest and prosecution.[26] Likewise, States employ surveillance technologies, which may also be AI-enabled, such as closed-circuit television cameras, body cameras and face recognition technologies, during public gatherings, often without ensuring that the requirements of proportionality, transparency and accountability are met.[27]

1. Use of AI systems by judges and lawyers

9. According to the Committee on Racial Discrimination, algorithmic risk assessments are sometimes used to assess the degree of risk posed by a person at different stages in the criminal justice process, for example, "[w]hen applying a sanction, or deciding whether someone should be sent to prison, be released on bail or receive another punishment".[28] There are also reports of judges using generative

---

[18] United Nations Educational, Scientific and Cultural Organization (UNESCO), *Global Toolkit on AI and the Rule of Law for the Judiciary* (Paris, 2023).

[19] Lorna McGregor, Daragh Murray and Vivian Ng, "International human rights law as a framework for algorithmic accountability", *International and Comparative Law Quarterly* (17 April 2019).

[20] A/74/335; A/HRC/43/46.

[21] OHCHR, "Landmark ruling by Dutch court stops government attempts to spy on the poor – UN expert", 5 February 2020; National Non-Discrimination and Equality Tribunal of Finland, "Assessment of creditworthiness, authority, direct multiple discrimination, gender, language, age, place of residence, financial reasons, conditional fine: Multiple discrimination in the assessment of creditworthiness", available at www.yvtltk.fi/en/index/opinionsanddecisions/decisions.html.

[22] United States District Court, Southern District of Texas, Houston Division, *Houston Federation of Teachers v. Houston Independent School District*, Opinion, 4 May 2017.

[23] A/HRC/43/29.

[24] A/75/590; A/HRC/48/31; A/HRC/48/76; University of Essex and OHCHR, "Digital border governance: a human rights based approach", September 2023.

[25] A/HRC/48/31.

[26] Submission from the Canadian Human Rights Commission.

[27] Such technologies have been used to crack down on peaceful protests; see A/HRC/44/24.

[28] CERD/C/GC/36.

AI to gain a more comprehensive understanding of the bail laws that apply in cases of assault,[29] to test the potential of generative AI for judicial decision-making in cases involving sexual offences[30] and to assist with sentencing.[31] In one Member State, prosecutors use AI to ask legal questions.[32] In another, "smart courts" have been established, which reportedly are pilot testing "AI judge" programmes that directly assist in rendering court decisions, under close human supervision and without the intention of replacing human judges.[33] That pilot programme has served to highlight the unreliability of certain AI systems, including facial and emotional recognition technology for validating whether testimony is credible.[34]

10. AI is also being used by some lawyers to expedite the drafting of legal documents and written court submissions. Given current statistical limitations, AI models may "hallucinate", or fabricate false outputs,[35] because they work by anticipating probable words with no grounding in reality or verifiable fact.[36] In such hallucinations, false, misleading or illogical information is generated and presented as facts, which could involve the fabrication of case law that does not exist. Some national courts are beginning to require lawyers and litigants to certify whether they used AI in drafting court filings.[37] Lawyers may also inadvertently share confidential client information with AI models.[38]

2. Impact of AI on human rights

11. AI systems have the potential to improve access to justice in many ways, including through digital case management systems, easier access to legal information using chatbots[39] and applications that assist investigations of crimes such as child sexual exploitation and abuse.[40] As highlighted by the High-level Advisory Body for Artificial Intelligence, AI systems may also pose risks for various rights due to the way such systems are developed or operated, as discussed below.[41]

Non-discrimination

12. According to United Nations human rights mechanisms, predictive policing tools used to identify potential future crimes can easily produce discriminatory

[29] Suman Shubhanshi, "ChatGPT: paving the way of AI into courtrooms", Legal Service India E-Journal.

[30] Courting the Law, "ChatGPT-4 Used in a Pakistani Judgment as an Experiment", 7 April 2023.

[31] "State v. Loomis: Wisconsin Supreme Court requires warning before use of algorithmic risk assessments in sentencing", *Harvard Law Review*, vol. 130, No. 5 (March 2017); Submission from the American University Paris Working Group.

[32] Submission from Qatar.

[33] Nyu Wang and Michael Yuan Tian, "'Intelligent justice': human-centred considerations in AI transformation", *AI Ethics*, vol. 3, no. 2 (2023).

[34] Submission from the International Bar Association Human Rights Institute.

[35] United States District Court, Southern District of New York, *Roberto Mata v. Avianca, Inc.*, Opinion and Order on Sanctions, 22 June 2023.

[36] First-Tier Tribunal (Tax Chamber) of the United Kingdom of Great Britain and Northern Ireland, *Felicity Harber v. The Commissioners for His Majesty's Revenue and Customs*, Case No. TC09010, Judgment, 4 December 2023.

[37] United States Court of Appeals for the Fifth Circuit, "Notice of proposed amendment to Fifth Circuit rule 32.3", available at www.ca5.uscourts.gov//docs/default-source/default-document-library/public-comment-local-rule-32-3-and-form-6; United States District Court for the District of Montana, Missoula Division, *David Belenzon v. Paws Up Ranch, LLC,* Order, 22 June 2023.

[38] Submission from the International Bar Association Human Rights Institute.

[39] Submission from Spain; submission from Justice with Children.

[40] Submission from the United Nations Office on Drugs and Crime (UNODC); UNICRI, "AI for safer children".

[41] High-level Advisory Body on Artificial Intelligence, "Interim report: governing AI for humanity", December 2023, available at https://www.un.org/techenvoy/ai-advisory-body.

outcomes; pose the risk of steering future predictions in the same, biased direction, leading to overpolicing of the same neighbourhood, which in turn may lead to more arrests in that neighbourhood, creating a dangerous feedback loop;[42] and may reproduce racial discrimination and gender biases.[43] In the view of the Committee on the Elimination of Racial Discrimination, the increasing use of new technological tools, including AI, in areas such as security, border control and access to social services, has the potential to deepen racial, gender and other types of multiple and intersecting forms of discrimination and exclusion, including against persons with disabilities.[44] United Nations human rights mechanisms have also expressed concerns about the use of facial recognition and other mass surveillance technologies by law enforcement agencies at peaceful assemblies, including in relation to the disproportionate impact the use of such technologies has on certain ethnic and racial groups.[45]

13. United Nations human rights mechanisms have also raised concern about the mandatory collection of extensive biometric data, including DNA samples, by law enforcement.[46] In some instances, DNA profiling has been used by law enforcement authorities to make false claims that certain ethnic minorities are more prone to violence, which has led, in turn, to those groups being subjected to discriminatory police practices.[47]

14. According to the Committee on the Elimination of Racial Discrimination, bias and discrimination may be embedded into algorithmic profiling systems when the data used include: information concerning protected characteristics under the Convention on the Elimination of All Forms of Racial Discrimination; information concerning socioeconomic factors that can serve as a proxy for discrimination, such as postal codes, educational attainment and mental health; data that are biased against a group;[48] and data that are poor quality because they have been poorly selected or are incomplete, incorrect, outdated or cannot be disaggregated for vulnerable populations, for instance, by sex and gender.

Liberty and security

15. According to the United Nations Educational, Scientific and Cultural Organization (UNESCO), in situations in which an individual's physical freedom or personal safety is at stake, such as with predictive policing, recidivism risk assessment and sentencing, use of AI might infringe upon that person's right to liberty, security and fair trial. The "black box" nature of AI systems makes it difficult for legal professionals, such as judges, attorneys and prosecutors, to understand the rationale behind the outputs of the system, which may complicate the justification and appeal of the decision. The opacity of AI systems might adversely affect the right to liberty and security if accused individuals are not able to challenge decisions affecting them. There are several documented cases in which the use of AI algorithms

[42] CERD/C/GC/36; A/HRC/44/57.
[43] CEDAW/C/DEU/CO/9; CEDAW/C/ITA/CO/8.
[44] CERD/C/GC/36.
[45] CCPR/C/GBR/CO/8; CERD/C/ITA/CO/21; CERD/C/BRA/CO/18-20; CERD/C/THA/CO/4-8; A/HRC/56/68; A/HRC/47/CRP.1; submission from Justice with Children; European Union Agency for Fundamental Rights, "Facial recognition technology: fundamental rights considerations in the context of law enforcement", 21 November 2019.
[46] CERD/C/CHN/CO/14-17; CCPR/C/120/D/2326/2013/Rev.1; European Court of Human Rights, *S. and Marper v. the United Kingdom*, Application Nos. 30562/04 and 30566/04, Judgment, 4 December 2008; OHCHR, "New and emerging technologies need urgent oversight and robust transparency: UN experts", 2 June 2023; submission from Citizen Lab.
[47] CERD/C/GC/36; A/HRC/41/35.
[48] CERD/C/GC/36; A/HRC/44/57; Julia Angwin and others, "Machine Bias", ProPublica, 23 May 2016.

in predictive policing, risk assessment and sentencing has led to suboptimal outcomes in the criminal justice system.[49]

16. According to the Human Rights Committee, the prohibition of arbitrary detention means that the decision to detain, or continue to detain, someone must be based on reasons specific to that individual. Detention pending trial must be based on an "individualized determination that it is reasonable and necessary taking into account all the circumstances for such purposes as to prevent flight, interference with evidence or the recurrence of crime".[50] The very nature of fully algorithmic decision-making, in which there is no human oversight, precludes the possibility of an individualized determination, as the final analysis is based on group behaviour, generalized statistical inferences and correlation rather than causation. If courts are to use algorithmic decision-making to facilitate decisions regarding detention, they must have the ability to obtain meaningful disclosures about, and develop an understanding of, algorithmic technologies, their functionalities, source code, training and input data.[51]

Equality before courts and fair trial

17. UNESCO is of the view that, when AI systems are biased and opaque, they raise concerns regarding fair trial standards, such as the presumption of innocence, the right to be informed promptly of the origin and nature of an accusation, the right to a fair hearing and the ability to defend oneself in person.[52] Under international human rights law, a fair hearing entails a right to equality of arms before the courts.[53] In civil proceedings, each side must be given the opportunity to contest the arguments and evidence adduced by the other party.[54] In criminal trials, the accused has a right to a defence[55] and must have adequate facilities for the preparation of that defence,[56] which includes access to documents and other evidence and must include all materials that the prosecution plans to offer in court against the accused or that are exculpatory.[57] These rights might be undermined in situations in which defendants are unaware that AI systems were used in making a decision that affected them, where defendants are unable to understand how AI systems reached the decision that was made, or where defendants are unable to challenge or appeal the decision-making process or the decision itself.[58] Lack of access to information can compromise the accused's right to an effective remedy, both during and after the completion of criminal proceedings against them.[59]

18. There are reports that digital evidence collected, sometimes unlawfully, by means of surveillance technologies, such as facial recognition technology, has been used in criminal proceedings to arrest, charge, prosecute and convict individuals involved in protests, as well as in their bail proceedings.[60] Such digital evidence can

[49] UNESCO, *Global Toolkit on AI and the Rule of Law for the Judiciary*.

[50] CCPR/C/GC/35.

[51] Kate Robertson, Cynthia Khoo and Yolanda Song, *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* (Toronto, Canada, Citizen Lab and the International Human Rights Program of the University of Toronto Faculty of Law, 2020).

[52] UNESCO, *Global Toolkit on AI and the Rule of Law for the Judiciary*.

[53] International Covenant on Civil and Political Rights, article 14.1.

[54] CCPR/C/GC/32; European Court of Human Rights, Second Section, *Sigurđur Einarsson and others v. Iceland*, application No. 39757/15, Judgment, 4 June 2019.

[55] International Covenant on Civil and Political Rights, article 14.3 (d).

[56] Ibid., article 14.3 (d).

[57] CCPR/C/GC/32; CCPR/C/CAN/CO/5.

[58] Fair Trials, "Automating injustice: the use of artificial intelligence and automated decision-making systems in criminal justice in Europe", 9 September 2021.

[59] International Covenant on Civil and Political Rights, article 2.

[60] Submission from Privacy International.

impact the right to a defence, as it is often gathered without transparency, making it difficult for the defence to challenge its accuracy, credibility and lawfulness. AI technology also opens up greater possibilities of forging evidence to incriminate individuals, threatening not only the right to privacy but fair trial rights and the presumption of innocence.[61]

Independence of the judiciary

19. The Special Rapporteur on the independence of judges and lawyers has expressed concerns regarding challenges to judicial independence linked to digital technologies and artificial intelligence.[62] Under international human rights law, tribunals are required to be competent, independent and impartial, and hearings must be public.[63] Tribunals must be independent of the executive and legislative branches of Government, and judges must enjoy judicial independence in deciding legal matters. A situation where the executive is able to control or direct the judiciary is incompatible with the notion of an independent tribunal.[64] Influence exercised by the executive or the legislature over, inter alia, the selection of the training data used to teach an AI system how to respond to questions or the design of the algorithm used in a courtroom could raise questions regarding the independence of the court,[65] especially in cases in which the design and implementation of the system are outsourced to private companies, particularly because control of AI currently tends to be concentrated in the hands of a small number of companies.[66]

20. According to UNESCO, one of the greatest threats arising from the use of AI systems in the administration of justice is the so-called automation bias, which is the tendency of humans to uncritically consider the solution offered by artificial intelligence as correct, thereby automatically validating the solution. This is a particularly aberrant risk in the administration of justice[67] and may render the human input in the system ("the human in the loop") ineffective.[68] Therefore, a judge's decision to deviate from any decision that is assisted or automated should not be subject to any form of reprisal, sanction, inspection or disciplinary regime.

21. AI systems or "AI judges" are incapable of applying equitable principles, instead reducing complex problems to mere matters of formalistic legality.[69] According to the United Nations Development Programme (UNDP), AI systems also lack empathy and discretion.[70] Decision makers can use their discretion to acknowledge systemic disadvantages and strengthen opportunities for rehabilitation. Systems that leave no room for discretion can lead to rigid and harsh results[71] and lack the innovation to create or diverge from precedents. As one member of the

[61] A/HRC/23/40; A/HRC/39/29; A/HRC/51/17.
[62] A/HRC/53/31.
[63] International Covenant on Civil and Political Rights, article 14; European Commission for the Efficiency of Justice, *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*, 4 December 2018.
[64] CCPR/C/GC/32.
[65] Stanley Greenstein, "Preserving the rule of law in the era of artificial intelligence (AI)", *Artificial Intelligence and Law*, vol. 30 (17 July 2021).
[66] Consultative Council of European Judges, "Moving forward: the use of assistive technology in the judiciary", opinion No. 26, 1 December 2023.
[67] UNESCO, *Global Toolkit on AI and the Rule of Law for the Judiciary*.
[68] Lorna McGregor, Daragh Murray and Vivian Ng, "International human rights law as a framework for algorithmic accountability".
[69] Submission from the International Bar Association Human Rights Institute.
[70] Submission from the United Nations Development Programme (UNDP).
[71] Ibid.

judiciary said, “judicial discretion is shaped not just by our legal training and experience, but our experiences as humans”.[72]

22. One legal scholar argues that individuals should have a right to challenge decisions made by or with the help of AI systems and supports a right to review by a human of such decisions or a right to have a human decide in the first instance. He draws attention to the dehumanizing effect of treating individuals merely as members of a group of similarly categorized individuals and not as full-fledged individuals endowed with human dignity.[73] Two other scholars reject the use of fully automated decision-making tools in international human rights adjudication but endorse the use of facilitated automatic decision-making for the purposes of formulating straightforward recommendations regarding the registration and admissibility of complaints, subject to an accountability framework.[74]

3. Emerging AI governance frameworks

23. Some Member States are establishing domestic frameworks for the use of AI by public and private actors. Most Member States lack an overarching legal and regulatory framework that specifically addresses the use of AI in the justice system. Such frameworks are often articulated as policies, rather than as laws, and thus do not create any legal obligations or provide for legal remedies.[75] The Federal Court of Canada has recognized the inherent risks of AI and has developed interim principles and guidelines for the court’s use of artificial intelligence. The European Commission for the Efficiency of Justice has also provided guidance for judicial professionals on the use of generative AI tools in work-related contexts.

24. The European Union, through its AI Act, has adopted a risk-based approach to regulating AI systems. The Act classifies AI systems intended for use by a judicial authority or on its behalf to assist with researching or interpreting facts and the law or with applying the law to a concrete set of facts as “high risk”. Pursuant to the Act, AI tools can be used to support the decision-making power of judges but should not replace it: decision-making must ultimately remain a human-driven activity. The Act prohibits the use of risk assessments to assess or predict risk of offending, based solely on the profiling of a person or assessing their personality traits and characteristics, and prohibits the use of real-time facial recognition technology in publicly accessible spaces for law enforcement purposes, with limited exceptions.[76] The Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, adopted by the Council of Europe on 17 May 2024, is aimed at ensuring that activities within the life cycle of AI systems are fully consistent with human rights, democracy and the rule of law. UNESCO, in its Recommendation on the Ethics of AI, underscores that States should enhance the capacity of the judiciary to make decisions related to AI systems, in line with international law and standards. It emphasizes that sufficient safeguards are needed to guarantee the protection of human rights, the rule of law, judicial independence and the principle of human oversight, as well as to ensure trustworthy, public interest-oriented and human-centric

[72] Submission from the International Bar Association Human Rights Institute.

[73] Yuval Shany, “The case for a new right to a human decision under international human rights law”, 4 November 2023.

[74] Veronika Fikfak and Laurence R. Helfer, “Automating international human rights adjudication”, *Michigan Journal of International Law*, vol. 45, No. 1 (2024) and *Duke Law School Public Law and Legal Theory Series* No. 2024-28 (12 April 2024).

[75] Submission from the Canadian Human Rights Commission.

[76] Laura Lazaro Cabrera and Iverna McGowan, “EU AI Act brief: part 1, overview of the EU AI Act”, Center for Democracy and Technology, 14 March 2024.

development and use of AI systems in the judiciary. It also clarifies that life and death decisions should not be ceded to AI systems.[77]

25. The High Commissioner for Human Rights recommends that States ban AI applications that cannot be operated in full compliance with human rights law and impose a moratorium on the sale and use of AI that carry a high risk for the enjoyment of human rights, unless and until adequate safeguards to protect human rights are in place.[78] The United Nations Office on Drugs and Crime (UNODC) has cautioned against the broader application of AI systems in the criminal justice system, including for predictive models and decisions or risk assessments.[79] In partnership with the International Criminal Police Organization, the United Nations Interregional Crime and Justice Research Institute has developed a "toolkit for responsible AI innovation in law enforcement"[80] as well as policy guidance on setting responsible limits on facial recognition technology.[81]

26. The High Commissioner has advocated for an advancement of AI grounded in human rights in the private sector through the application of the Guiding Principles on Business and Human Rights and through the B-Tech project.[82] The High-level Advisory Body on Artificial Intelligence has formulated preliminary recommendations on international AI governance and has proposed a global AI governance framework, which would include human rights impact assessments by private- and public-sector developers of AI systems.[83]

B. Digital technologies in prisons

27. An increasing number of prison services are developing digital rehabilitative programmes and security solutions, often with the support of regional and national policies and legislation.[84] Virtual reality is being used by, among others, prison psychologists to rehabilitate a range of criminal behaviours, with the aims of improving thinking and positive social skills and the ability to empathize, increasing motivation to engage in rehabilitation and boosting well-being and relaxation.[85]

28. Technologies for maintaining security in prisons are also being developed, ranging from the use of AI and facial recognition technology in response to violence to the use of mobile phone blockers, body scanning equipment and biometrics.[86] There have been reports of prisoners in solitary confinement on death row being

[77] A/HRC/48/31; UNESCO, "Recommendation on the ethics of artificial intelligence", 16 May 2023; Council of Europe, "Council of Europe framework convention on artificial intelligence and human rights".

[78] A/HRC/48/31.

[79] Submission from UNODC.

[80] UNICRI and INTERPOL, "Toolkit for responsible AI innovation in law enforcement".

[81] INTERPOL and others, "A policy framework for responsible limits on facial recognition: use case – law enforcement investigations", November 2022.

[82] OHCHR, "B-Tech project: OHCHR and business and human rights", available at www.ohchr.org/en/business-and-human-rights/b-tech-project.

[83] Envoy of the Secretary-General on Technology, "High-level Advisory Body on Artificial Intelligence", available at www.un.org/techenvoy/ai-advisory-body. Some States also undertake human rights impact assessments, see the submissions from Albania, Czechia, Guatemala and Spain.

[84] Penal Reform International and Thailand Institute of Justice, *Global Prison Trends 2023* (London and Bangkok, June 2023).

[85] Pia Puolakka, "The purpose of digitalization of prisons is rehabilitation and reintegration", Reshape, 15 January 2024; Carlos Fernández Gómez, "A new approach for open prisons in Spain", EuroPris, 10 March 2023, available at https://www.europris.org/file/feature-article-a-new-approach-for-open-prisons-in-spain-2023/.

[86] Submission from Penal Reform International.

subjected to 24-hour surveillance, with no measures to ensure their privacy while using the toilet or changing their clothes.[87] The Committee against Torture recommends the installation of closed-circuit television surveillance and body cameras in places of deprivation of liberty, except where doing so would give rise to violations of the detainees' right to privacy or the confidentiality of their conversations with their counsel or doctor. The Committee has raised concerns about the placement of prisoners under constant video surveillance in their cells.[88] UNODC is digitalizing risk and needs assessment tools for prisons that incorporate human rights considerations and audit toolsets based on the United Nations Standard Minimum Rules for the Treatment of Prisoners (the Nelson Mandela Rules) for use in Kazakhstan, Kyrgyzstan and Tajikistan.[89]

C. Electronic monitoring

29. Electronic monitoring is a general term referring to forms of surveillance that are used to monitor the location, movement and specific behaviour of persons and the collection and analysis of certain data. Methods of electronic monitoring currently in use are based on radio wave, biometric or satellite tracking technology. Electronic monitoring usually involves a device, such as an ankle monitor or smartphone, being attached to a person and monitored remotely.[90] In the criminal justice process, such monitoring is generally used to prevent absconding, as an alternative to pretrial detention or imprisonment, as part of probation, and as a means of tracking and monitoring people in detention settings and in the migration context.[91] Evidence suggests that the use of electronic monitoring is on the rise.[92] Business enterprises may drive the uptake of electronic monitoring, including the uptake of specific models for that purpose, and may play a central role in the delivery of those models, including through public-private partnerships.[93]

Impact of electronic monitoring on human rights

30. The Human Rights Committee and the Committee against Torture support the use of electronic monitoring as one alternative to detention, alongside parole, community service and release.[94] Detention pending trial should, however, be an exception, not a rule, so as to protect the presumption of innocence. Thus, electronic monitoring should only be used as an alternative to detention pending trial when grounds for such detention exist. Detention pending trial must be based on an individualized determination that, taking into account all the circumstances, detention is reasonable and necessary for such purposes as to prevent flight, interference with evidence or the recurrence of crime.[95] When electronic monitoring is employed without grounds for detention, the scope of surveillance is widened to include low-

[87] Center for Prisoners Rights, "End solitary confinement and video surveillance of death row prisoners", 22 August 2022, available at https://prisonersrights.org/english/.
[88] CAT/C/AZE/CO/5, para. 17 (d); CAT/C/KAZ/CO/4; CAT/C/ITA/CO/5-6; CAT/C/ROU/CO/3, para. 14 (d).
[89] Submission from UNODC.
[90] Council of Europe Committee of Ministers, recommendation CM/Rec(2014)4 on electronic monitoring.
[91] University of Essex and OHCHR, "Digital border governance: a human rights based approach"; Doughty Street, "Upper tribunal gives judgment in first challenge to Home Office policy of GPS tagging migrants", 12 March 2024.
[92] Submission from the American Civil Liberties Union.
[93] Submission from the University of Essex.
[94] CAT/OP/MKD/1; CCPR/C/BEL/CO/5; CCPR/C/KAZ/CO/1; CCPR/C/TUR/CO/1; CCPR/C/GC/35.
[95] CCPR/C/GC/35.

risk people, to the detriment of other approaches, such as community-based rehabilitation.[96]

31. The Committee against Torture has expressed regret at the requirement that those subject to monitoring have to pay for electronic monitoring devices, noting that this may have a discriminatory impact on indigent persons.[97] Research suggests that, in some countries, certain groups may be disproportionately subject to electronic monitoring; that some forms of electronic monitoring can impede access to education, work and the delivery of care-giving responsibilities; and that such monitoring can result in deprivations of liberty where the device fails, is defective or cannot be charged due to homelessness.[98] When used in situations where there are no grounds for detention, there is a risk that electronic monitoring may constitute an unlawful and arbitrary interference with the right to privacy of both the wearer and the people with whom they live and interact. The design and implementation of electronic monitoring devices may also fail to take into account the needs of women and persons with disabilities.[99]

32. While the United Nations Standard Minimum Rules for Non-custodial Measures (the Tokyo Rules) do not explicitly relate to electronic monitoring, they provide guidance on the use of non-custodial measures, including in relation to systematic evaluation and observance of human rights, such as the right to privacy of the person monitored and their family. In addition, pursuant to the Tokyo Rules, non-custodial measures should be prescribed by law, consent must be obtained from the person monitored and there must be the possibility of judicial review. The United Nations system common position on incarceration supports implementation of non-custodial measures. UNODC developed a feasibility study on the use of electronic monitoring bracelets in Kyrgyzstan, which influenced legislative changes to adopt electronic monitoring as an alternative to pretrial detention,[100] and the Office of the United Nations High Commissioner for Human Rights (OHCHR) advised on the necessary human rights safeguards. The Council of Europe has adopted recommendations enabling national authorities to provide just, proportionate and effective use of different forms of electronic monitoring, in full respect of the rights of the persons concerned.[101] Morocco has adopted a law regulating the use of electronic monitoring devices.[102] Some stakeholders are of the view that there is an international protection gap, highlighting the need for greater guidance by international human rights bodies on the human rights compatibility of electronic monitoring models.[103]

D. Digital technologies in court administration

33. States are increasingly using case management systems to streamline administrative processes within the justice system, including systems for electronic case filing, record-keeping, monitoring of proceedings, identification of the parties, payment of fees, delivery of documents, communication with the parties to proceedings, storage of audio or visual recordings and greater accessibility for

[96] See the submissions from the University of Essex, Penal Reform International and the American Civil Liberties Union.

[97] CAT/C/GTM/CO/7.

[98] Submission from the University of Essex.

[99] See the submissions from the American Civil Liberties Union, the University of Essex and Penal Reform International.

[100] Submission from UNODC.

[101] Council of Europe Committee of Ministers, recommendation CM/Rec(2014)4.

[102] Submission from Morocco.

[103] See the submissions from Penal Reform International and the University of Essex.

persons with disabilities.[104] Search engines for national and international jurisprudence are also being used. Where automated forms of proceedings are in use, they are used in low value civil proceedings (small claims) and to facilitate judgments and other court decisions in simple procedural matters.[105] The use of AI in court administration remains at an early stage of development,[106] and applications tend to be focused on administrative tasks, such as dictation, translation and automatic anonymization of judgments and orders.[107]

34. UNDP, in its Strategic Plan 2022–2025 and its Digital Strategy 2022–2025, provides a set of guiding principles for digital transformation, including a human rights-based approach.[108] Under that plan, the biggest area of UNDP support for e-justice pertains to digital case management systems and tools for court registries, in-court access to case files and evidence, court filing systems and legal aid services, including in Albania, Bangladesh, Brazil, Chad, Côte d'Ivoire, the Democratic Republic of the Congo, Djibouti, El Salvador, Fiji, Kenya, Malawi, Maldives, Morocco, Senegal, Sierra Leone, Ukraine and the State of Palestine.[109]

35. In Pakistan, UNDP and OHCHR provided technical assistance to strengthen the harmonization of data collection and reporting on human rights and the Sustainable Development Goals through a digital platform.[110] In Libya, OHCHR supported the reform of the criminal justice system and prosecutorial services by enhancing digitalization.[111] In Cambodia, OHCHR supported the development of a criminal case database for storing and tracking data and provided training to staff on its use. In Bolivia, the information management system supported by the United Nations Children's Fund (UNICEF) serves all parties to criminal proceedings; the system is a model for the region and has received awards for technical innovation.[112] UNODC supported information and communications technology reforms in the justice sector in Kenya, including reforms focused on the integration of electronic filing systems across different bodies.[113] In Kyrgyzstan, UNODC enhanced criminal justice information management through the unified registry of crimes and implemented automated information systems as part of the "Justice for all" programme.

36. States and United Nations entities have attested to the potential of digital technologies for court administration in terms of greater access to justice, transparency, accessibility, auditability, expeditiousness and efficiency for all parties. Efficiency should not, however, be conflated with high-quality outcomes. An efficient system that reduces costs to the user but results in unenforceable decisions, exacerbates the gender digital divide[114] or fails to protect rights is not an improvement.[115]

---

[104] As reported by most States in their submissions. See also the submissions from the Azerbaijan Human Rights Commission and the Netherlands Institute for Human Rights; European Commission for the Efficiency of Justice, *European Judicial Systems: CEPEJ Evaluation Report – Part 1, Tables, Graphs and Analyses* (Strasbourg, France, 2022).

[105] Consultative Council of European Judges, "Moving forward: the use of assistive technology in the judiciary"; submission from Czechia.

[106] Consultative Council of European Judges, "Moving forward: the use of assistive technology in the judiciary".

[107] Consultative Council of European Judges, "Moving forward: the use of assistive technology in the judiciary"; submission from the Canadian Human Rights Commission.

[108] UNDP, "Justice: digitalization and e-justice".

[109] A/79/117; submission from UNDP.

[110] A/79/117.

[111] Ibid.

[112] Submission from UNICEF.

[113] Submission from UNODC.

[114] CEDAW/C/BTN/CO/1.

[115] UNDP, *E-Justice: Digital Transformation to Close the Justice Gap* (New York, 2022).

Impact of the use of digital technologies in court administration on human rights

37. Digital technologies should not have negative impacts on or jeopardize the independence of the judiciary.[116] Where implementation of technological reform is solely the responsibility of the executive, the independence of the judiciary may be at risk (see paras. 18–21 above). The use of data tools to develop performance indicators for judicial case management involving the imposition of efficiency-based targets could run counter to the autonomy of judicial decision-making. The same is true where the oversight of technology used by the judiciary is carried out by the executive branch or a regulatory body, instead of by a body within the judiciary itself. Thus, in order to secure judicial independence, the judiciary must have a role and responsibility in the implementation of digital reform.[117]

38. The right to equality of arms (see para. 17 above) in criminal proceedings also requires that the defence benefits from full access to digital case management systems and digitalized case files.[118] If this condition is satisfied, efforts to reduce reliance on paper files, which require physical access, thereby limiting the time available for their inspection, can have an important impact on the daily work of defence lawyers, potentially reducing delays and improving the quality of legal assistance.[119] The right to privacy could potentially be affected by digital case management systems, as such systems constitute a repository of personal and sensitive information. Protection of the right to privacy requires robust legislative and regulatory frameworks that are aligned with the right to privacy and data protection principles.[120]

39. Many States have legislation regulating certain areas of digital technologies in the field of cybersecurity and data handling, transfer and protection, under which case management systems are also regulated. States within the European Union must comply with the General Data Protection Regulation, and some have additional legislation. In some States, supreme courts have issued decisions on the use of digitalized court management systems and issued agreements regulating the judicial management thereof. With the assistance of UNDP, legislative amendments have been or are being developed as part of digital transformation projects in Antigua and Barbuda, Barbados, Belize, Brazil, Dominica, Guyana, Saint Lucia, Saint Kitts and Nevis, Trinidad and Tobago, Morocco and the State of Palestine. Those amendments are focused on access to and handling and storage of electronic data, access restrictions, and control and ownership of court-related data and processes.[121]

E. Online hearings

40. Since the coronavirus disease (COVID-19) pandemic, there has been an increase in the use of online hearings–judicial hearings conducted using videoconferencing or a hybrid format in which some participants attend virtually. States avail themselves

[116] European Commission for the Efficiency of Justice, “Guidelines on electronic court filing (e-filing) and digitalization of courts”, 9 December 2021.

[117] Consultative Council of European Judges, “Justice and information technologies (IT)”, opinion No. (2011)14, 9 November 2011; European Commission for the Efficiency of Justice, “Guidelines on electronic court filing (e-filing) and digitalization of courts”.

[118] Fair Trials, “Briefing paper on the communication on digitalization of justice in the European Union”, January 2021.

[119] Sergio Carrera, Valsamis Mitsilegas and Marco Stefan, *Criminal Justice, Fundamental Rights and the Rule of Law in the Digital Age: Report of a CEPS and QMUL Task Force* (Brussels, Centre for European Policy Studies, May 2021).

[120] Submission from UNODC; Personal Data Protection and Privacy Principles, see https://unsceb.org/sites/default/files/imported_files/UN-Principles-on-Personal-Data-Protection-Privacy-2018_0.pdf.

[121] Submission from UNDP.

of such technology at different stages of the criminal justice process, from investigation to appeal, and in cross-border cooperation. UNDP and UNODC have assisted in the establishment of virtual courts in Kenya and Pakistan, and OHCHR has advised Kyrgyzstan on human rights safeguards for online hearings.[122]

Impact of online hearings on human rights

41. Many Member States and United Nations entities attest to the benefits of online hearings, which can facilitate the participation of some or all parties and thus have the potential to increase access to justice; improve efficiency; generate cost-savings; remove logistical barriers in gaining access to court facilities;[123] reduce the demand for physical space;[124] provide greater flexibility for the legal profession;[125] reduce travel and carbon dioxide emissions;[126] and enhance accessibility.[127] There is evidence that videoconferencing is beneficial for vulnerable complainants, such as those affected by gender-based violence, and witnesses for the prosecution, and it has been recommended by the Human Rights Committee for all cases in which it is necessary to safeguard the rights of both the accused persons and the victims or the victims' relatives, particularly in cases where the physical presence of any of the parties would endanger their lives.[128]

42. While online hearings can enhance efficiency and cost-effectiveness, they should only be implemented when regulations are in place to ensure the protection of human rights, fair trial guarantees and the existence of safeguards.[129] One supreme court judge concluded that "justice is done best in-person", while others have maintained that physical hearings should be the standard and judges should decide whether an online hearing may be organized.[130] The European Court of Human Rights has stated that: "it must be ensured that the applicant is able to follow the proceedings and to be heard without technical impediments, and that effective and confidential communication with a lawyer is provided for."[131]

43. There are no specific international standards on online hearings, which are subject to generally applicable standards for due process and fair trial.[132] Human rights treaty bodies have expressed the view that custody hearings should be held in the physical presence of the detainee to prevent and ensure accountability for torture or ill-treatment.[133] The Human Rights Committee has referred to the right to be brought promptly to appear "physically" before a judge once a person has been arrested or detained, to ensure judicial control of detention, which is a right without exception. If continued detention is then ordered, detainees have the right to appear in person before the court to challenge the legality of the detention under the habeas corpus principle.[134] With

[122] A/79/117.
[123] Submission from UNODC.
[124] Submission from Mexico.
[125] Submission from Nigeria.
[126] Submission from Spain.
[127] Submission from Mexico.
[128] CCPR/C/COL/CO/8, para. 29 (b); Commission on Crime Prevention and Criminal Justice, "The impact of COVID-19 on criminal justice system responses to gender-based violence against women: a global review of emerging evidence", 28 April 2021; submissions from Czechia, Estonia, Morocco, Nigeria and Serbia; submission from the University of Sydney Law School.
[129] A/HRC/47/35; submissions from Colombia and the India National Human Rights Commission.
[130] Submissions from the University of Sydney Law School and the Netherlands Institute for Human Rights.
[131] European Court of Human Rights, First Section, *Sakhnovskiy v. Russia*, application No. 21272/03, judgment, 5 February 2009.
[132] CCPR/C/GC/32.
[133] CAT/C/BRA/CO/2; CCPR/C/BRA/CO/3.
[134] CCPR/C/GC/35.

respect to both judicial control of detention and habeas corpus applications, the physical presence of the detainee is, in principle, essential, as signs of torture or ill-treatment cannot be observed properly on a screen and the ability to complain of ill-treatment may be compromised if an individual is heard online from a place of detention.

44. As for other criminal hearings, the accused has the right to be tried in their presence, and trials must be conducted orally and publicly.[135] Thus, trials of criminal cases should only be held online with the explicit free and informed consent of the accused, subject to respect for due process guarantees.[136] OHCHR has developed guidance for online hearings, as has the European Commission for the Efficiency of Justice of the Council of Europe.[137]

45. While there are recognized advantages of online hearings for persons with disabilities, persons with disabilities must enjoy procedural accommodations and accessibility rights in such hearings. Persons with disabilities face additional barriers, as digital applications are not generally designed with persons with diverse types of impairment in mind and are often designed without their participation. If technology is used in criminal proceedings, supported decision-making measures must be made available to those persons with disabilities who need such measures, so that they can exercise their legal capacity and access to justice in line with international law, including the Convention on the Rights of Persons with Disabilities.[138] When digital technologies are used for hearings involving defendants with psychosocial disabilities or cognitive impairments, the defendants must be ensured access to supported decision-making and other procedural accommodations, to avoid systemic exclusion and to ensure that they can understand the case and the language of the court and communicate effectively and confidentially with their legal representatives.[139]

46. Many agree that some of the benefits of online hearings for children can reinforce their rights, such as improving access to justice and release from detention following minor charges,[140] protecting them from harm and revictimization, increasing participation of family members and witnesses, allowing access by legal aid organizations to remote areas and potentially reducing anxiety online.[141] UNICEF is supporting States in the use of technology for receiving testimony and evidence from children.[142] Nevertheless, online hearings pose significant risks. Beyond the exacerbation of inequality and discrimination owing to the digital divide, and the privacy issues related to unauthorized access and the storage of personal information, the child's right to participate effectively may be affected by a lack of human contact in an online hearing. Such hearings may also undermine lawyer-client communication, affecting trust and the capacity to provide adequate support and assistance. Other concerns include the difficulty for the judiciary to fully assess the physical appearance and demeanour of the child and confirm the safety and confidentiality of the setting from which the child is calling in. For these reasons, several civil society

[135] CCPR/C/GC/32.

[136] CCPR/C/111/D/2041/2011; CCPR/C/GC/35; submission from the Netherlands Institute for Human Rights; Constitutional Council of France, decision No. 2020-872 QPC, 15 January 2021.

[137] OHCHR, "Online hearings in justice systems", 2 August 2023; European Commission for the Efficiency of Justice, "Guidelines on videoconferencing in judicial proceedings", 17 June 2021.

[138] Submission from the Validity Foundation.

[139] Submission from the University of Sydney Law School; OHCHR, Special Rapporteur on the rights of persons with disabilities, "International principles and guidelines on access to justice for persons with disabilities", OHCHR, 15 August 2019.

[140] UNICEF, in its submission, refers to the release of over 5,000 children from detention as a pandemic mitigation measure in Bangladesh.

[141] J. Davidson and others, "Justice for children policy brief: digital justice for children – innovation, risks and advantages", Justice for children policy brief series, 2023.

[142] Submissions from Mexico, Uganda and UNICEF.

organizations express the view that in-person court proceedings should be the norm for proceedings involving children, supported by remote technologies.[143]

47. There is a lack of data and research analysing the impact of online hearings on the human rights of children. The Committee on the Rights of the Child recommends regularly updated data and research to understand the implications and impact of the digital environment on children.[144] Concerns have also been expressed about the use of privately owned platforms in sensitive government settings, which presents serious data collection and privacy questions.[145]

F. Neurotechnology

48. In 2021, in his report entitled "Our Common Agenda", the Secretary-General indicated that consideration should be given to updating or clarifying the application of human rights frameworks and standards to address frontier issues and prevent harms in the digital or technology spaces, including in relation to neurotechnology.[146] Neurotechnology applications are "those devices and procedures used to access, monitor, investigate, assess, manipulate and/or emulate the structure and function of the neural systems of natural persons".[147]

49. Most of the neurotechnology applications being proposed in the criminal justice system are extremely problematic from a human rights perspective. Examples of applications being researched include brain-based lie detection, the retrieval of eyewitness testimonies through "memory recovery" and determination of the risk of reoffending.[148]

50. Outside the medical field, the use of neurotechnology is operating outside a common regulatory regime. Some Member States have advanced legislation or declarations to protect neural data and the people it is collected from, while others are in the process of doing so. The Organisation for Economic Co-operation and Development has adopted recommendations in this area, and UNESCO has launched a standard-setting process, to be finalized in November 2025.[149] The Advisory Committee to the Human Rights Council will present a study on the impact of neurotechnology on human rights to the Council at its fifty-seventh session. The Secretary-General has called for "robust standards for mental integrity, mental privacy and mental freedom" and "clearer guidelines governing the application of neurotechnology".[150]

---

[143] Submissions from the Alana Institute and Justice with Children.

[144] CRC/C/GC/25; submission from the Alana Institute.

[145] Submission from the Alana Institute.

[146] A/75/982, para. 35

[147] OECD, recommendation of the Council on Responsible Innovation in Neurotechnology, OECD/LEGAL/0457, 10 December 2019.

[148] A/76/380; Milena Costas Trascasas, "Impact, opportunities and challenges of neurotechnology with regard to the promotion and protection of all human rights", available at www.ohchr.org/en/hr-bodies/hrc/advisory-committee/session31/index; Australian Human Rights Commission, "Protecting cognition: background paper on human rights and neurotechnology", March 2024; submission from the Neurorights Foundation.

[149] See UNESCO, Records of the General Conference, forty-second session, 42 C/resolution 29.

[150] Secretary-General of the United Nations, "Message to the UNESCO International Conference on the Ethics of Neurotechnology", 13 July 2023.

IV. Conclusions and recommendations

51. **Digital technologies and AI systems are increasingly being used throughout the administration of justice, including by judges and lawyers, in law enforcement and investigation, in case file management, to conduct online hearings, in the prison context and as an alternative to detention. The United Nations is working with States to explore how some of these technologies can be deployed to improve the administration of and access to justice. However, the application of digital technologies and AI systems in the administration of justice also has the potential to negatively impact human rights, notably in criminal justice, and those who are in vulnerable situations are likely to be disproportionately affected. The unregulated, inappropriate and improper use of such technologies can contribute to serious violations of human rights, including the rights to liberty and security, freedom from torture and ill-treatment, fair trial by an independent judiciary, access to legal remedies, non-discrimination and privacy. The potential use of neurotechnology in the administration of criminal justice also raises concerns.**

52. **The present report is not a comprehensive review of this complex issue but should serve to highlight the latest developments, challenges and good practices in human rights in the administration of justice. The nature of the system into which digital technologies and AI systems are introduced, criminal justice policy and the roles and effectiveness of monitoring and oversight bodies may further affect the protection of human rights. Owing to the pace of growth of these technologies, serious analysis and assessment of their possible impacts on human rights are required, and regulation of their use must also keep apace.**

53. **The present report has served to highlight actual and potential gaps in human rights protection, including in relation to the use of AI by law enforcement, in courts and by the judiciary and the legal profession, as well as gaps in the conduct of online hearings, in the use of electronic monitoring and in the use of neurotechnology.**

54. **I recommend that Member States:**

(a) **Consider implementing the recommendations set out by the High Commissioner in her report on the right to privacy in the digital age (A/HRC/48/31), including the recommendation for States and business enterprises to systematically conduct human rights due diligence throughout the life cycle of AI systems, particularly comprehensive human rights impact assessments, as has also been recommended by the General Assembly in its resolution 78/213;**

(b) **Regulate, on the basis of a human rights framework, the development, deployment and use of digital technologies and AI in the administration of justice by law enforcement, courts and members of the legal profession as well as the development of such technologies by business enterprises or other entities;**

(c) **Refrain from or cease the use of AI applications that are impossible to operate in compliance with international human rights law, including predictive policing applications, profiling and surveillance models such as biometric identification systems, and in the judiciary, including in judicial decisions in criminal cases and in recidivism risk assessments for bail and parole decisions, unless and until the responsible authorities can demonstrate that such applications are in compliance with the right to a fair trial, including an independent judiciary, and the rights to liberty and security, non-discrimination, freedom from torture and ill-treatment and privacy, as well as other affected**

human rights, and that the authorities have addressed the disproportionate negative impact that the use of these technologies can have on specific groups;

(d) **Ensure that AI systems are designed to and deployed in such a way to produce explainable, non-discriminatory results; ensure accessibility for persons with disabilities; and ensure that vulnerable groups, such as women and persons with disabilities, are included in the development, deployment, use and oversight of such systems;**

(e) **Consider enacting laws to regulate AI systems used in law enforcement and in legal proceedings, with clear guidelines, standards and safeguards that comply with international human rights law; and ensure that the judiciary has an oversight role and responsibility in the development, deployment and use of digital technologies, and that there are regulations to protect its independence;**

(f) **Ensure that there are robust data protection laws aligned with the right to privacy where digital technologies and AI are employed in the administration of justice;**

(g) **Ensure that public-private partnerships for the provision and use of digital technologies and AI in the administration of justice are transparent and subject to human rights oversight carried out by bodies that are independent from the public authorities and private entities that are developing, deploying or otherwise using the AI systems;**

(h) **Consider including, in reports to United Nations human rights treaty bodies and the universal periodic review, as appropriate, information on the design, use and deployment of digital technology and AI in their justice systems, with a view to encouraging greater transparency, oversight and guidance on the compatibility of such technology with human rights;**

(i) **Ensure the provision of training and education to police, judges, lawyers and other legal professionals to ensure that technology, including AI and biometric technologies, is only used in the administration of justice when such use is in compliance with human rights;**

(j) **Conduct public awareness campaigns on the human rights and legal implications of technology in the justice system, including through the fostering of dialogue and consultations with affected communities and stakeholders;**

(k) **Increase the transparency of use of AI by States, courts and businesses, including by adequately informing the public and affected individuals and enabling independent and external auditing of automated systems. The more likely and serious the potential or actual human rights impacts linked to the use of AI are, the more transparency is needed;**

(l) **Undertake further independent research on the human rights impacts of online hearings, in particular for vulnerable groups such as women, persons with disabilities and children, and on the practical measures needed to ensure that such hearings comply with human rights, notably the right to a fair trial and the right to be free from arbitrary detention, torture and ill-treatment.**

55. **I recommend that Member States and courts:**

(a) **Ensure that the use of digital technologies and AI conforms with the right to a fair trial, judicial independence and impartiality and the right to liberty and security of person, that such use does not reproduce or aggravate discrimination and that parties to legal proceedings are made aware of any use of AI in those proceedings, understand its impact and have the opportunity to challenge its use;**

(b) **Ensure that electronic monitoring is only used as an alternative to detention pending trial when grounds for detention exist and ensure respect for human rights in any use of such monitoring;**

(c) **Ensure that digital evidence is collected in a transparent and regulated manner, with appropriate safeguards, before being introduced in judicial proceedings and that the members of the judiciary and legal representatives involved in criminal proceedings are trained and equipped appropriately to interrogate and weigh digital evidence;**

(d) **Ensure that courts and members of the legal profession store and manage all data in a secure technological environment, in which the right to privacy of all parties to the proceedings is protected and confidentiality is preserved, as appropriate.**

56. **I recommend that businesses take all steps to meet their responsibility to respect human rights through operationalization of the Guiding Principles on Business and Human Rights.**