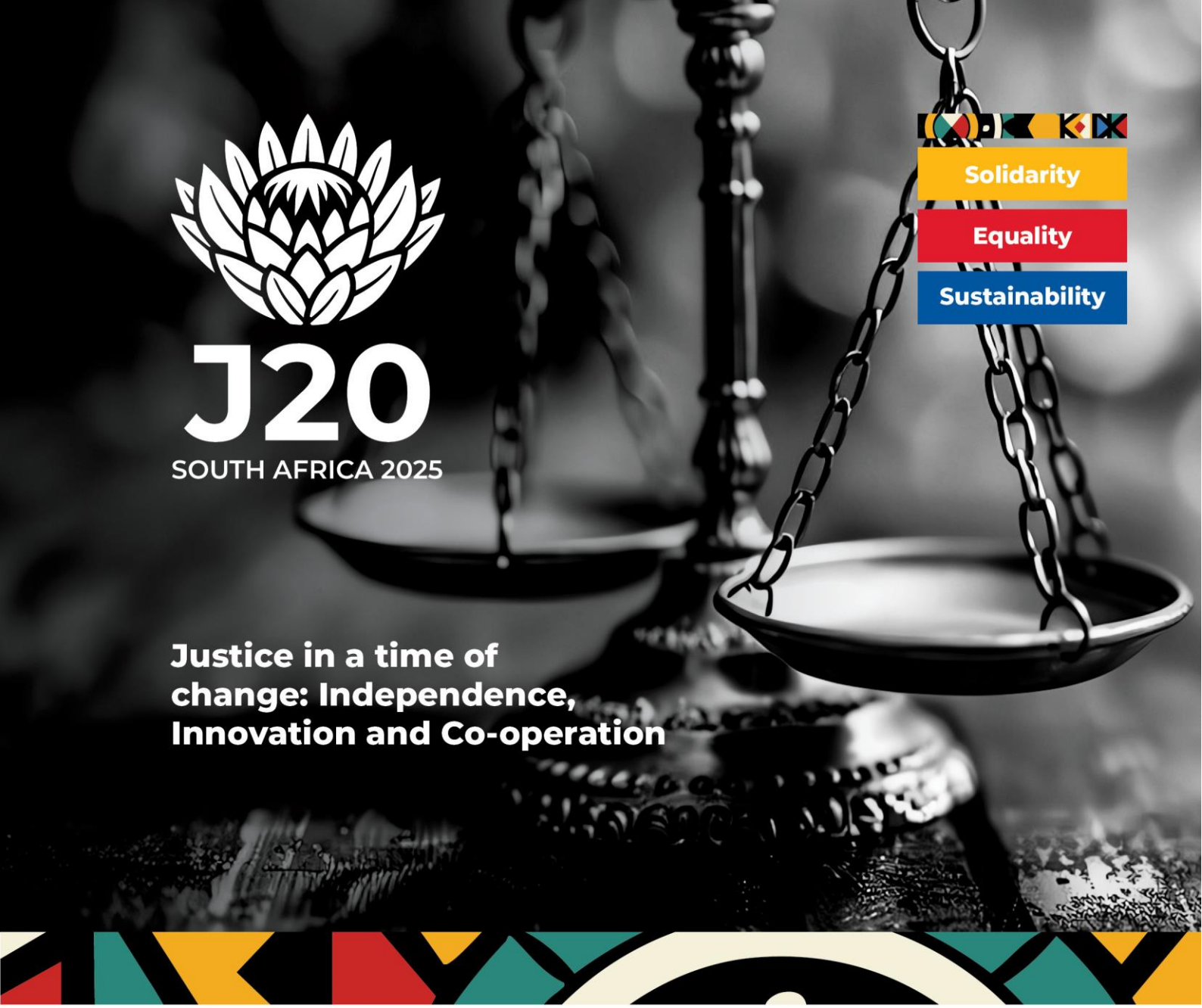

J20 Briefing Papers

3-4 August 2025

Johannesburg, South Africa

G20 SOUTH AFRICA 2025

unesco

juta

South Africa
Inspiring new ways
www.southafrica.net

#J20SouthAfrica | #ReKaofela | www.j20.judiciary.org.za

Table of Contents

J20
SOUTH AFRICA 2025

Solidarity
Equality
Sustainability

BRIEFING PAPER: Day 1 Plenary Session 1

Advancing Judicial Independence and Accountability: Preserving the Rule of Law and reinforcing judicial security in an evolving legal landscape

#J20SouthAfrica | #ReKaofela | www.j20.judiciary.org.za

Justice in a time of change: Independence, Innovation and Co-operation

G20
SOUTH AFRICA 2025

unesco

juta

South Africa
Inspiring new ways
www.southafrica.net

BRIEFING PAPER: Day 1 Plenary Session 1

Advancing Judicial Independence and Accountability: Preserving the Rule of Law and reinforcing judicial security in an evolving legal landscape

Contents

Advancing Judicial Independence and Accountability: Preserving the Rule of Law and reinforcing judicial security in an evolving legal landscape

> "Our constitutional system depends on judges who can make decisions without fear of reprisal or retribution. This is essential not just for the safety of judges and their families, but also to protect our democracy."[1]

Introduction

Advancing judicial independence and accountability through multifaceted measures is essential for the integrity of the Judiciary. The measures contribute to a strong, resilient, and trusted judiciary. Judicial independence is the cornerstone of a functioning democracy.

Globally, the Judiciary is a critical arm of government as it plays an important role in protecting and upholding constitutional democracy, enforcing the rule of law and vindicating fundamental rights.[2] The Constitution provides that judicial authority is vested in the courts, which are independent and subject only to the Constitution and the law.[3] The courts are enjoined to apply the law impartially and without fear. To achieve this, preserving the rule of law and reinforcing judicial security is critical.

Judicial independence is the fundamental requirement for upholding the rule of law, it is a principle that safeguards abuse of power and arbitrariness in a democracy. One of the key

---

1 Letter to Senate Appropriations Committee (United States) signed by Judge John Lungstrum, and Judge Roslynn Mauskopf (7 June 2021), available at https://www.uscourts.gov/file/33275/download

2 *S v Van Rooyen (General Council of the Bar of South Africa Intervening)* [2002] ZACC 8; 2002 (5) SA 246 (CC); 2002 (8) BCLR 810 (CC) at para 17; *South African Association of Personal Injury Lawyers v Heath* [2000] ZACC 22; 2001 (1) SA 883 (CC); 2001 (1) BCLR 77 (CC) at para 31; *In re: Certification of the Constitution of the Republic of South Africa* [1996] ZACC 26; 1996 (4) SA 744 (CC); 1996 (10) BCLR 1253 (CC) at para 123; *Pheko v Ekurhuleni Metropolitan Municipality (Socio-Economic Rights Institute of South Africa as Amicus Curiae) (No 2)* [2015] ZACC 10; 2015 (5) SA 600 (CC); 2015 (6) BCLR 711 (CC) at paras 26-7; and *De Lange v Smuts NO* [1998] ZACC 6; 1998 (3) SA 785 (CC); 1998 (7) BCLR 779 (CC) at para 47. In specific, the Judiciary is the ultimate protector of all fundamental rights – see *South African Association of Personal Injury Lawyers v Heath* [2000] ZACC 22; 2001 (1) SA 883 (CC); 2001 (1) BCLR 77 (CC) at para 46.

3 s 165(1) and (2) of the Constitution of The Republic of South Africa 1996, provide that: 'The judicial authority of the Republic is vested in the courts. The courts are independent and subject only to the Constitution and the law, which they must apply impartially and without fear, favour or prejudice'.

requirements of the rule of law is that the courts be independent and free of political interference from the executive or any other source. The true measure of the independence of the Judiciary lies in the way it relates to the executive and other organs of state in practice.

Generally, Judiciaries grapple with balancing judicial independence and accountability in practice. There is some perception that judicial independence implies a lack of judicial accountability, hence unsatisfactory judicial performance in some instances.[4] There is a need for the J20 participants to unpack judicial independence and judicial accountability and further engage in how a balance can be struck to maintain the equilibrium.

Judicial security is a fundamental component of a democratic society; without it, judicial independence becomes hollow.[5] Judicial decisions increasingly place members of the Judiciary at odds with litigants and broader segments of society, contributing to a heightened risk to their personal safety and security. These are in the form of physical attacks, cyberattacks, stalking, harassment, targeted and incidental threats. Where the Judiciary works under threat, judicial independence and public trust are compromised.

The secure functioning of court infrastructure is a prerequisite for both judicial continuity and the principle of open justice. Sustained and strategic investments in infrastructure, personnel, and integrity safeguards are necessary to ensure the safety of all stakeholders in the judicial process. Improving judicial infrastructure and promoting continuing judicial education are key components of reforming judicial independence.

The aim of the session is to discuss key issues relating to advancing judicial independence and accountability, reinforcing institutional independence, judicial security and the rule of law. Aspects discussed under judicial security are judicial security of tenure, physical security and cyber-security as it relates to Judges. Through innovation and judicial cooperation, it is possible to bring about reforms that foster judicial independence, enhance access to justice, and ensure public trust.

4 S Colbran, “The limits of Judicial Accountability: The Role of Judicial Performance Evaluation” (2003) 6 (1) *Legal Ethics* 55 - 72.

5 JP McGill “Upholding Justice under threat: The critical importance of judicial safety and security” (August 2025) *Michigan Bar Journal*.

Challenges

While legal frameworks may exist to advance judicial independence, reinforce judicial security and preserve the rule of law, the practical realities reveal a complex interplay of challenges as listed below:

a. *Financial constraints*: Judiciaries are faced with budget constraints. They opt to raise funds from external funding agencies therefore making the Judiciary vulnerable to implicit or explicit interference, going against the very essence of judicial independence. Resources are linked to exercise of judicial functions as they influence the state of available judicial infrastructure, facilities, and services rendered at the court. Without adequate number of Judges and supporting officials, dysfunctional equipment, and lack of personal security for the Judges, access to justice is compromised.

b. *Political pressure on appointments, removal, and other matters*: In some jurisdictions, the executive and legislative branches exercise undue influence or unfettered powers over the appointment of Judges and related matters. It is indeed unheard of for a Judiciary to determine the suitability of a member of the executive unless there is litigation. In some jurisdictions like South Africa and Kenya, legislation empowers political parties to remove Judges after considering recommendations from Judicial Services bodies or Tribunal. In Mongolia and Poland, the legislation provides that Judges are not removable subject to certain conditions.

c. *Judicial security of tenure*: It is a fundamental principle of judicial independence and accountability. There are different models of tenure, namely, life tenure and fixed term tenure. Judges may be appointed until a compulsory retirement age or for life subject to appropriate judicial conduct. Judges who leave the bench due to retirement age may still be fit to work and might look for other work opportunities. This could make them vulnerable to undue influences. In contrast, Judges on life tenure with no age limit may be on the bench until their death provided that their mental faculties are not declining. For example, Judge Oliver Holmes was 91 years old when he retired from the US Supreme Court, and Justice Ruth Bader Ginsburg was still in active service when she passed on at the age of 87 years.[6]

[6] Supreme Court of Historical Society accessed at https://supremecourthistory.org/associate-justices/oliver-wendell-holmes-jr-1902-1932/ 26 August 2025; J Biskupic and A de Vogue (2020) September 19 CCN https://edition.cnn.com/2020/09/18/politics/ruth-bader-ginsburg-dead (accessed 26 August 2025).

d. *Judicial Security*: Enhanced use of technology or digitisation may lead to unintended consequences if safeguards put in place are not robust enough. For example, providing personal profiles of members of the Judiciary on websites or the internet tends to increase vulnerability to threats and attacks by dissatisfied litigants and or members of the community.

Judicial Security as key component to judicial independence and the rule of law

The personal safety of Judges and magistrates is vital to the effective administration of justice, ensuring judicial independence and empowering judicial officers to make decisions free from fear or intimidation.[7] There have been a number of reported instances of actual physical assaults, violent attacks, or murders of sitting Judges or magistrates in South Africa in recent years.

In 2019, a plea was made for increased protection for judicial officers, indicating "numerous incidents" where judicial officers had been threatened, including the locking down of the High Court when judgment was handed down by a Judge whose life had been threatened.[8] In 2021, an article authored by Judges Matter, a South African civil society organisation established to promote transparency and accountability in the Judiciary, raised concerns about threats to judicial safety, which prompted the Office of the Chief Justice (OCJ) to tighten security at Judges' homes and court buildings.[9]

Building and Maintaining Courts as Safe Spaces

First, it is crucial to gather and use information to anticipate and manage risks. This includes robust systems for collecting and sharing data on potential threats, developing safety plans in advance of hearings (especially highly sensitive ones). This process needs to be participatory with input from architects, security personnel, court staff, and the Judiciary to collaborate and

---

7 **Challenges for judicial independence and impartiality in the member states of the Council of Europe** Report prepared jointly by the Bureau of the CCJE and the Bureau of the CCPE (15 January 2016) p 18, available at https://rm.coe.int/sginf-2016-3rev-challenges-judicial-independence-/16807778b9. See also John F. Muffler and Judge James R. Brandlin Judicial Security Recommendations For Implementing Sound Protective Intelligence Methodologies available at https://www.ncjfcj.org/wp-content/uploads/2022/03/aba-judicial-security-protective-intel.pdf

8 C Richard Top Judge Pleads For Protection of Judicial Officers (14 June 2019) available at https://africanlii.org/articles/2019-06-14/carmel-rickard/top-judge-pleads-for-protection-of-judicial-officers.

9 JudgesMatter Judges Matter Praises Judicial Independence and Condemns Unfair Criticism and Threats Against Judges in South Africa (21 July 2021) available at: https://www.judgesmatter.co.za/press-releases/judges-matter-praises-judicial-independence-and-condemns-unfair-criticism-and-threats-against-judges-in-south-africa/.

discuss anticipated risks and safety concerns.[10] Databases, operational notes, and photographs can be exchanged to ensure open lines of communication between all affected parties.

Security measures put in place at the courts must therefore be proportionate, integrated and designed to avoid a punitive or exclusionary atmosphere. Overly carceral environments marked by visible weaponry, imposing fortifications, and intrusive screening, can discourage attendance, especially among marginalised groups and self-represented litigants.[11]

The courthouse should signal transparency and civic engagement through its physical form while discreetly incorporating protection at every level. This can be achieved through:

a. Transparent facades and open sightlines that allow observation of public spaces without compromising security.[12]

b. Strategic location of screening areas just inside entrances, where they are visible enough to signal safety but designed to preserve dignity and minimise bottlenecks.[13]

c. Multiple entry points for different user groups (Judges, in-custody defendants, public) to reduce confrontation risks.[14]

Courthouses are civic spaces. Security should be embedded in their architecture in a manner that maintains their symbolic roles as places of justice. Passive measures such as open sightlines, natural surveillance, and inviting public spaces can complement active measures like access control and screening. By embedding these elements into a coherent design strategy, courts can protect all users, uphold the dignity of proceedings, and sustain public trust, ensuring that delivery of justice remains both safe and accessible.

---

10 R Sarre & A Vernon "Access to Safe Justice in Australian Courts: Some Reflections upon Intelligence, Design and Process" (2013) 2 IJCJ 133 at 146. ("Such [security] changes also demonstrate the growing awareness of the interrelationship between court security and the overall objectives of justice processes – and the importance of balancing a range of interests and needs of those attending and working within the court environment.").

11 L Mulcahy "Architects of Justice: the Politics of Courtroom Design" (2007) 16 Social and Legal Studies 383. See also K L Jesmore "The Courthouse Search" (1973) 21 UCLA Law Review at 797.

12 R Sarre & A Vernon "Access to Safe Justice in Australian Courts: Some Reflections upon Intelligence, Design and Process" (2013) 2 IJCJ 133 at 141.

13 As above: R Sarre & A Vernon "Access to Safe Justice in Australian Courts: Some Reflections upon Intelligence, Design and Process" (2013) 2 IJCJ 133 at 139.

14 M Griebel & T S Phillips "Architectural Design for Security in Courthouse Facilities" (2001) 576 American Academy of Political and Social Science 118 at 121.

A secure and inclusive courthouse requires careful circulation design. Spatial organisation plays a decisive role in balancing safety with openness. Secure circulation routes for Judges and staff should connect directly to courtrooms without intersecting with public areas. In-custody defendants should be transported via enclosed, restricted corridors that lead directly to secure holding rooms adjacent to courtrooms.[15] Public routes should be clearly marked, intuitive, and easy to navigate, with a logical layout that avoids unnecessary bottlenecks. Vertical and horizontal separation of public, restricted, and high-security zones should be reinforced by controlled doorways and lifts.[16] These design features reduce the potential for security breaches while ensuring that members of the public, including those with disabilities, can move through the space confidently and independently.

Security outside the courthouse or court buildings is equally important. Setback zones between the building and surrounding streets provide space for surveillance and controlled vehicle access. Bollards, planters, and other landscape features can protect against vehicle-borne threats without creating a fortress-like appearance. Designated pedestrian drop-off points and accessible parking close to entrances make arrival safe and convenient. Adequate exterior lighting and discreet camera coverage enhance safety without creating a sense of being under constant surveillance.[17]

Inside the courthouse, security and openness must coexist in the courtroom and public spaces. Examples from newer courts show that replacing glass barriers with sit-down counters can reduce hostility, and that creating flexible, well-furnished waiting areas in calming colours enhances psychological safety.[18] Design should allow for separate entrances and exits for opposing parties, safe rooms for vulnerable users, and child-friendly spaces in courts handling family matters. Even in heritage buildings, retrofitting wireless surveillance, controlled access, and reconfigured spaces can address safety gaps. Courtroom layouts should preserve clear lines of sight for public observation while maintaining safe separation. Duress alarms should be installed in all high-contact areas, including public counters and witness stands. Waiting

15 M Griebel & T S Phillips “Architectural Design for Security in Courthouse Facilities” (2001) 576 American Academy of Political and Social Science 118 at 121.

16 O O Makinde “Spatial and Security Organisation of Court Buildings: An Assessment of Selected High Court Buildings in Nigeria” (2020) available at:https://www.researchgate.net/publication/348204586_Spatial_and_Security_Organisation_of_Court_Buildings_An_Assessment_of_Selected_High_Court_Buildings_in_Nigeria.

17 M Griebel & T S Phillips “Architectural Design for Security in Courthouse Facilities” (2001) 576 American Academy of Political and Social Science 118 at 121.

18 R Sarre & A Vernon “Access to Safe Justice in Australian Courts: Some Reflections upon Intelligence, Design and Process” (2013) 2 IJCJ 133 at 139.

areas should have good visibility, sufficient seating, and arrangements that allow opposing parties to avoid direct, unsupervised contact. Public amenities such as restrooms and information counters should be located within secure but freely accessible zones.[19]

Strategies and Systems for Safety on Courts

The following list of specific measures, created by consolidating the measures that other countries have in place or have proposed, may be considered to improve judicial security:

a. Assessment of the security systems in place at courts.[20]

b. Establishment of a central Threat Management Centre to monitor and investigate threats to judicial officers.[21]

c. Creation of guiding principles for measures Judges can take to ensure their own security inside and outside the courts.[22]

d. Ensuring that personal security for Judges outside the court are strengthened through measures such as home audit programmes,[23] and regular updates and improvement of **home security systems**.[24]

Accessibility as a Security Imperative

Accessibility is not an optional supplement to security; it is integral to it. Step-free entrances and automatic doors at public entry points help ensure that mobility is not impeded. Tactile paving, braille signage, and auditory wayfinding assist those with visual impairments, while

---

19 *Ibid* at 138.

20 See Steps to Best Practices for Court Building Security report issued by the National Centre for State Courts (February 2010) available at https://www.ncjfcj.org/wp-content/uploads/2022/03/best-practices-for-court-building-security.pdf

21 Such as that operated by the United States Marshall Service (USMS): see Judicial Security 2024 Fact Sheet, available at https://www.usmarshals.gov/sites/default/files/media/document/2024-Judicial-Security.pdf

22 See for example National Centre for State Courts Personal safety tips for judges and court staff (Updated October 2023), available at https://www.ncsc.org/sites/default/files/media/document/personal-safety-tips-judges-court-staff-2023.pdf. See also John F. Muffler and Judge James R. Brandlin Judicial Security. Recommendations for implementing sound protective intelligence methodologies available at https://www.ncjfcj.org/wp-content/uploads/2022/03/aba-judicial-security-protective-intel.pdf and R Zayas Staying Safe: Five steps judges can take now (2025) available at https://judicature.duke.edu/articles/staying-safe-five-steps-judges-can-take-now/

23 See National Center for State Courts Home Security Audit and Recommendations (Revised June 2013), available at: https://ncsc.contentdm.oclc.org/digital/collection/facilities/id/173/

24 These is one of the suggestions that the judiciary put to Congress in 2020. See United States Court "Congress Urged to Adopt Judicial Security Measures" (9 September 2020) available at https://www.uscourts.gov/data-news/judiciary-news/2020/09/09/congress-urged-adopt-judicial-security-measures.

hearing augmentation systems in courtrooms enable meaningful participation for individuals with hearing loss. Clear sightlines and colour-contrasted signage help those with cognitive or sensory processing difficulties to navigate the space without confusion. These measures prevent security infrastructure from becoming a barrier to participation and instead position it as an enabler of safe, equal access.

Security also depends on resilient operational infrastructure. Reliable electricity, telecommunications, and climate control are essential to keeping courts open and functioning. Power failures can halt hearings, disable screening equipment, and compromise safety systems, while telecommunications outages can disrupt remote proceedings and internal coordination. To prevent such disruptions, courts should incorporate backup power systems, and, where possible, local energy generation with storage.[25] These systems not only maintain operations during emergencies but also support transparency by ensuring proceedings remain visible and accessible. Infrastructure resilience is thus a core component of courthouse security, safeguarding both physical safety and the continuous, participatory functioning of justice.

Courthouses are civic spaces. Security should be embedded in their architecture in a manner that maintains their symbolic roles as places of justice. Passive measures such as open sightlines, natural surveillance, and inviting public spaces can complement active measures like access control and screening. By embedding these elements into a coherent design strategy, courts can protect all users, uphold the dignity of proceedings, and sustain public trust, ensuring that delivery of justice remains both safe and accessible.

Cyber Security and the Judiciary

In executing its mandate, the South African judicial system is reliant on digital infrastructure, for example the CourtOnline platform and emails for improved case management, efficient communication, and enhanced public access to legal services.[26] The digitisation of court operations through the integration of digital technologies has improved procedural efficiency

---

25 M Griebel & T S Phillips “Architectural Design for Security in Courthouse Facilities” (2001) 576 American Academy of Political and Social Science 118 at 129 (“In the event of a power disruption, an emergency power generator should automatically operate key lights, heat/smoke and duress alarms, the public address system, and other essential operating equipment in the facility. Status monitoring of the emergency generator should be provided in the building central control area. In addition to the facility emergency power system, uninterruptible power supply and standby batteries should be provided for the security system.”).

26 South African Judiciary “CourtOnline” available at: https://www.judiciary.org.za/index.php/63-caselines?start=3

and access to courts. This transformation was accelerated by the COVID-19 pandemic, which necessitated the adoption of virtual hearings and other remote legal processes.[27] However, this digital transformation encompasses with it, significant risks in relation to cybersecurity, for example ransomware attacks, unauthorised access to sensitive judicial information and data breaches.[28]

Fortunately, South Africa has a rather robust legal framework governing cybersecurity.[29] One of these instruments is the Cybercrimes Act[30] which criminalises unlawful access, data interference, and cyber fraud, and provides law enforcement with the authority to investigate and seize digital evidence. The Cybercrimes Act is complemented by the Protection of Personal Information Act (POPIA) ,[31] the POPIA, which requires institutions such as courts to implement reasonable safeguards to protect personal data and notify the Information Regulator in case of any breaches. Additionally, the Electronic Communications and Transactions Act[32] outlines offences related to unauthorised access and data interception, reinforcing the legal framework for secure digital operations. As an institution, the Office of the Chief Justice is responsible for the administration of superior courts. It is a vital role-player in overseeing the digital transformation of judicial processes. At this stage, the Department of Justice and Constitutional Development has a responsibility for broader justice sector IT systems and must ensure compliance with cybersecurity legislation. This equips the Judiciary with the necessary tools to detect, investigate and protect our institutions. Once the envisaged court-led administration model is adopted for purposes of achieving institutional independence, all aspects pertaining to all the courts in South Africa will be administered by the Judiciary.

Although the shift toward digital systems has had significant advantages, it has also introduced new layers of complexity and potential security gaps that require attentive oversight. Given the inherently sensitive nature of the Judiciary's infrastructure, it is imperative to implement robust cybersecurity strategies to safeguard the judiciaries electronic and cyber infrastructure

27 Renato Solimar Alves et al "Enhancing cybersecurity in the judiciary: Integrating additional controls into the CIS framework" Computer and Security 2025.

28 As above: Renato Solimar Alves et al "Enhancing cybersecurity in the judiciary: Integrating additional controls into the CIS framework" Computer and Security 2025.

29 Schoeman Law Inc 'Understanding South African cybersecurity law in the context of the recent SAA cyber incident' available at https://www.polity.org.za/article/understanding-south-african-cybersecurity-law-in-the-context-of-the-recent-saa-cyber-incident-2025-07-31

30 19 of 2020.

31 4 of 2013.

32 25 of 2002.

from malicious threats. As the Judiciary becomes digitised, its vulnerability to cyber-attacks grows. In light of this, there is a need to ensure a high standard of cybersecurity, not only in relation to the protection of data but in preserving the integrity of the justice system and maintaining public confidence in the Judiciary's operations. Therefore, judicial bodies must adopt a proactive and strategic approach to mitigating risks by implementing rigorous information and data protection measures.

Another common challenge is the lack of or rather limited adequate technological infrastructure within the justice systems, including the limited availability of computer equipment, reliable and fast internet access, and secure data storage systems. Without a strong electronic and cyber infrastructure, achieving successful implementation of electronic processes can be challenging.

Having regard to the growing cybersecurity threats facing judicial institutions, experts, such as Rast,[33] emphasise that there is an urgent need for a comprehensive and proactive approach to digital security. He advocates for the implementation of robust technical safeguards and organisational practices that collectively strengthen the justice system's digital infrastructure. The adoption of multi-factor authentication is an example of a measure that can be implemented; it can significantly reduce the risk of unauthorised access as it requires multiple forms of identity verification. In addition, the use of Virtual Private Networks is also recommended to secure remote connections and protect sensitive data during transmission. These recommendations align with South Africa's broader legal obligations under the POPIA, the Cybercrimes Act, and the National Cybersecurity Policy Framework.

33 C Rast "Cybersecurity Threats to the Judiciary" (2023) available at: https://www.americanbar.org/groups/judicial/publications/judges_journal/2023/summer/cybersecurity-threats-to-judiciary/

Reflection Questions:

a. What are innovative ways of advancing judicial independence with the aim of preserving the rule of law and reinforcing effective judicial security.
b. How can judiciaries achieve independence that allows them to have complete control over judicial matters?
c. How can the judiciaries be protected against implicit external influences of executives, political parties, and donor agencies?
d. What are the most pressing security threats facing Judges and judicial personnel in your country?
e. Which effective measures have been implemented to protect Judges from intimidation, threats, or harassment?

Conclusion

There is considerable support around the globe for rule of law reform, and the international community can take considerable comfort from the progress made in some jurisdictions. But there is still a long way to go. Civil unrest and conflict in almost every continent mean that many disputes are still not being settled by peaceful means, so that the rule of force will decide the outcome, not the rule of law.

The fragility of the rule of law is evident even in more developed nations, where public attacks on the Judiciary threaten the integrity of our constitutional system. So, the best safeguard will have to be the unrelenting proactive efforts of the legal profession, the Judiciary, non-governmental organisations and institutions to promote the rule of law and judicial independence. Of necessity, this will need to be reinforced by all governments with the resources to do so, to achieve universal “freedom, justice and peace in the world in the next century”.

J20
SOUTH AFRICA 2025

Solidarity
Equality
Sustainability

BRIEFING PAPER: Day 1 Plenary Session 2

Balancing Artificial Intelligence Innovation with Fundamental Freedoms in the Judicial System

#J20SouthAfrica | #ReKaofela | www.j20.judiciary.org.za

Justice in a time of change: Independence, Innovation and Co-operation

G20
SOUTH AFRICA 2025

unesco

juta

South Africa
Inspiring new ways
www.southafrica.net

BRIEFING PAPER: Day 1 Plenary Session 2

Balancing Artificial Intelligence Innovation with Fundamental Freedoms in the Judicial System

AI in the Judiciary

1. Introduction

Artificial Intelligence (AI)[34] offers new opportunities and creates new risks for courts and legal professionals. At last year's J20 in Brazil, leaders examined how technology is supporting judicial transformation, such as AI powered tools which process thousands of appeals and screen cases for broader legal significance. These advances underscore the need for safeguards and risk management to ensure that the integration of AI in the judiciary remains safe, transparent, and consistent with human rights.

Continuing this momentum, the J20 in South Africa focuses on moving beyond viewing AI as a simple technical solution. Instead, jurisdictions are beginning to adopt comprehensive AI strategies that enhance the efficiency of the judicial process. This shift requires more than just updating technology or streamlining processes – it demands thoughtful consideration of AI's role in supporting, not supplanting, human judgment and judicial independence while respecting human rights and due process protections. Also, it is important to consider alternative solutions that require less personal data or less computing power and therefore a lower ecological footprint.

Accordingly, this Issue Brief explores two priority questions: What strategies best guide the responsible development and governance of AI within the Judiciary? And how does AI affect judicial independence? The brief first highlights prevailing trends and core elements of effective AI strategies in courts, drawing on international examples and institutional

[34] UNESCO, Recommendation on the Ethics of Artificial Intelligence, 2024, https://unesdoc.unesco.org/ark:/48223/pf0000381137?posInSet=7&queryId=c131b185-84ba-4e4d-8a28-94ecfdb2ffba, p.10, understands AI systems as "systems which have the capacity to process data and information in a way that resembles intelligent behaviour, and typically includes aspects of reasoning, learning, perception, prediction, planning or control." ; See also, OECD (2024), "Explanatory memorandum on the updated OECD definition of an AI system", OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris, https://doi.org/10.1787/623da898-en., "a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

safeguards. It then examines AI's broader implications for judicial independence, concluding with recommendations and questions for further reflection by Chief Justices.[35]

2. Key trends on AI use in the Judiciary

The use of AI in the Judiciary reflects a complex landscape marked by both rapid technological adoption and fragmented ethical and regulatory initiatives. This occurs against a context in which many judicial systems are overburdened with heavy caseloads, backlogs, and increasingly demanding cases involving complex and extensive repositories of digital evidence.

1. **Generative AI is increasingly used by judicial actors worldwide.** Judges, court staff, prosecutors, and lawyers increasingly use large language models (LLMs) to assist with the drafting of legal documents, judicial decisions, and courtroom arguments across a range of legal areas including administrative, criminal, constitutional, family, and privacy law. According to a UNESCO survey of judicial personnel in 96 countries,[36] 43% use generative AI to research legislation, jurisprudence, and doctrinal sources, while 28% are employing it for drafting and summarizing texts, emails, and legal arguments. Additional common uses include translating documents, transcribing testimony, and adapting materials for specific formats or presentations. Notably, 14% of respondents also use AI for brainstorming and exploring new legal ideas. This broad adoption highlights AI's growing role in managing workloads, enhancing efficiency, and supporting legal reasoning in courts around the world. It is worth considering that AI integration and uses come with a series of risks, including bias, data leakage and ecological impact that must be weighed against benefits, such as the efficiency gains.

35 This brief does not cover judicial decisions regarding AI use by external actors in areas like elections, expression, or labour and privacy rights, which are covered in more detail in the UNESCO Global Toolkit on AI and the Rule of Law, https://unesdoc.unesco.org/ark:/48223/pf0000387331?posInSet=1&queryId=79a0f42f-61f4-40bc-bf4a-4d9c8d1af7ba

36 UNESCO Global Judges' Initiative: survey on the use of AI systems by judicial operators, 2024, https://unesdoc.unesco.org/ark:/48223/pf0000389786

- In Argentina, judges have used LLMs to summarise their decisions in plain and accessible language.

- Law firms, legal service companies, and universities have developed GenAI systems based on LLMs, independently or with tech companies, to conduct legal research and litigation work, add context to a case, summarise legal texts, and draft emails and contracts. Judges and lawyers can thus use LLMs designed exclusively to carry out legal activities and other open-source LLMs.

- Problematically, reports have surfaced from Australia, Brazil, Canada, South Africa, Spain, and the United States regarding judges and lawyers who have issued judicial decisions or submitted legal documents that contained references to non-existent rulings due to the inappropriate use of AI chatbots.

Sources: UNESCO, Guidelines for the Use of AI in Courts and Tribunals, May 2025, p.5 https://unesdoc.unesco.org/ark:/48223/pf0000393682

Box 1 Use cases of generative AI by judges and lawyers

2. **Judiciaries at all levels are actively piloting and, in some cases, deploying AI tools to tackle distinct courtroom challenges.** Adoption is often led by court leadership collaborating with local innovators. AI systems are being developed and used for two functions:
    1. **Administrative tasks:** The Supreme Court of India deployed SUVAS, a software that translates thousands of documents from English into ten local languages and vice versa.[37] In France, the Court of Appeal of Paris[38] and the Tribunal of Strasbourg[39] are testing commercial AI solutions for legal research and case matching, while the Court of Cassation has developed tools to anonymise decisions, triage appeals, and analyse similarities and differences between cases.[40]
    2. **Legal analysis**: In Brazil, the Supreme Court implemented VICTOR, a system that processes thousands of appeals brought to the court and facilitates the

37 UNESCO, Guidelines for the Use of AI in Courts and Tribunals, May 2025, p.4 https://unesdoc.unesco.org/ark:/48223/pf0000393682

38 Cour d'appel de Paris, L'intelligence artificielle au cœur de la révolution judiciaire, June 13, 2025, https://www.cours-appel.justice.fr/paris/lintelligence-artificielle-au-coeur-de-la-revolution-judiciaire

39 Christian Licoppe, L'IA au tribunal : comment les magistrats s'approprient les outils de « justice prédictive » ?, IM Tech (Institut Mines Télécom), September 25, 2024, https://imtech.imt.fr/2024/09/25/lia-au-tribunal-comment-les-magistrats-sapproprient-les-outils-de-justice-predictive/

40 Cour de Cassation, « Cour de cassation et intelligence artificielle : préparer la Cour de demain », April 28, 2025, https://www.courdecassation.fr/files/files/Publications/IA%20-%20Rapport%202025/Rapport_IA_2025_Web.pdf

identification of cases that meet the "general repercussion" prerequisite.[41] In India, the Kerala High Court launched "ONCOURTS",[42] a 24/7 digital court, to streamline cheque bouncing disputes through online filing, hearings, and judgment delivery.

These examples demonstrate a growing commitment to targeted, practical AI innovation beyond the highest courts, focused on efficiency, transparency, and better justice outcomes.

3. **Lack of IT infrastructure, data, and human resource capacities remain major obstacles to AI development and use**. Successful, systemic integration of AI in courts depends on having a clean and solid database of digitised court decisions and legislation, adequate technological infrastructure, strong data management practices, and skilled personnel to develop, deploy, evaluate, and maintain safe, secure, and trustworthy AI systems underpinned by robust data governance and data protection safeguards. Without these foundational elements, AI initiatives in the judiciary risk remaining isolated pilot projects with indeterminate efficacy and safety, rather than delivering wide-ranging transformation and long-term impact. Judicial systems should prioritise investment not only in digital infrastructure, but as importantly in staff digital competence,[43] data governance,[44] and gender-responsive approaches that empower women in judicial digital transformation.[45] This is critical for scaling safe, fair, and accurate AI solutions and ensuring that the integration of technology is sustainable and improves existing judicial processes. Finally, separation of powers and judicial independence make it essential that decisions about personnel and the deployment of AI within the Judiciary remain at the sole discretion of the Judiciary.

4. **Non-profit organizations are developing AI solutions for courts.** Facing persistent challenges such as limited access and systemic delays, technology innovators with a social mission are driving the development of open-source AI solutions for courts. In the Netherlands, The Hague Institute for Innovation of Law (HiiL) partners with legal professionals to create people-centered digital tools for resolving everyday justice

41 UNESCO, Guidelines for the Use of AI in Courts and Tribunals, May 2025, p.4.
42 https://oncourts.kerala.gov.in/
43 UNESCO, Artificial intelligence and digital transformation: competencies for civil servants, 2022, https://unesdoc.unesco.org/ark:/48223/pf0000383325
44 UNESCO, Data governance toolkit: navigating data in the digital age, 2025, https://unesdoc.unesco.org/ark:/48223/pf0000394518?posInSet=1&queryId=65cd54fc-701d-48b4-9964-26cd2111f77e
45 UNESCO, Challenging systematic prejudices: an investigation into bias against women and girls in large language models, 2024, https://unesdoc.unesco.org/ark:/48223/pf0000388971 ; See also, UNESCO, Guidelines for the Use of AI in Courts and Tribunals, 2025, p.13, 16.

problems.[46] India's Agami[47] builds a broad community of judges, lawyers, and technologists, developing AI-powered platforms like OpenNyAI[48] and JIVA to enhance legal research and case management. These efforts illustrate how non-governmental actors are accelerating justice innovation and empowering users through practical and scalable open-source technology.

5. **AI development in the justice sector is increasingly shaped by new regulations at global, regional, and national levels**. Since 2016, more than thirty countries have enacted laws referencing AI, and legislative activity surged in 2024.[49] Courts and initiatives using AI must comply with this evolving landscape. Notably, the EU AI Act designates as "high risk"[50] any AI system intended to assist judicial authorities in researching, interpreting, or applying the law, including use in alternative dispute resolution. This status imposes strict requirements: deployers must establish risk management frameworks and maintain human oversight of these tools, ensuring accountability and responsible deployment.

The High Commissioner for Human Rights has recommended that States ban AI applications incompatible with human rights law, and impose a moratorium on high-risk AI unless adequate safeguards are in place. This position was echoed by the UN Secretary-General, who stressed that in the justice sector such restrictions should apply to AI in criminal adjudication and in risk assessments for bail and parole, unless authorities can demonstrate full compliance with fair trial guarantees, judicial independence, liberty, security, non-discrimination, privacy, and protection from torture and ill-treatment, while addressing disproportionate impacts on vulnerable groups. Importantly, the Secretary-General underscored that AI in justice must be regulated strictly within the human rights framework.

Source: UN, The right to privacy in the digital age - Report of the United Nations High Commissioner for Human Rights, A/HRC/48/31, September 2021 https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high and UN, Human rights in the administration of justice – Report of the Secretary-General, A/79/296, August 2024 https://docs.un.org/en/A/79/296

Box 2: UN reports on AI, Human Rights and Administration of Justice

46 HiiL, Justice Dashboard, https://dashboard.hiil.org/
47 Agami, https://www.agami.in/
48 OpenNyAI, https://opennyai.org/
49 UNESCO, Consultation paper on AI regulation: emerging approaches across the world, 2024, p.4, 14-17 https://unesdoc.unesco.org/ark:/48223/pf0000390979
50 EU AI Act, Art. 6 (Classification rules for high-risk AI systems), Recital 61 (High-risk AI systems in the administration of justice).

6. **Formal guidance on the use of AI tools in the justice sector remains limited.** A UNESCO survey found that while 44% of judicial operators – including judges, prosecutors, and lawyers – use AI tools like ChatGPT, only 9% have received institutional training or guidelines.[51] Only a handful of judiciaries have published official principles or guidelines on the ethical and responsible use of AI, including Argentina, Australia, Brazil, Canada, Colombia, New Zealand, Singapore, the United Kingdom, and the United States.[52] These documents outline expectations and best practices for both court staff and external court users, but most countries still lack comprehensive, sector-specific guidance for judicial actors.

7. **Capacity building for the judiciary on AI remains limited, even as judges increasingly face cases related to AI technologies.** Integrating AI into judicial decision-making introduces systemic risks, including potential discrimination and restricted access for marginalised groups. At the same time, the growth of AI in societies means more disputes involving human rights – such as privacy, liberty and security, freedom of expression, equality before the courts, fair trial, and protection against discrimination – will come before the courts. To meet these dual challenges, regular and comprehensive training is essential for judges and court staff. Capacity building should focus on developing digital literacy, understanding the legal, ethical and human rights impacts of AI,[53] and critically assessing AI-generated outputs in line with international human rights standards.[54]

3. Developing an AI Strategy for the Judiciary

The integration of AI into judicial systems offers significant opportunities to enhance justice delivery, efficiency, and people-centered approaches, provided that the Judiciary remains in control of the entire process. To benefit from this technology, G20 Judiciaries may consider

51 UNESCO Global Judges' Initiative: survey on the use of AI systems by judicial operators, 2024, https://unesdoc.unesco.org/ark:/48223/pf0000389786

52 See Annex for references.

53 UNESCO, Global Toolkit on AI & the Rule of Law for the Judiciary, 2023, https://unesdoc.unesco.org/ark:/48223/pf0000387331?posInSet=1&queryId=79a0f42f-61f4-40bc-bf4a-4d9c8d1af7ba ; see also, Recommendation on the Ethics of Artificial Intelligence, 2024, https://unesdoc.unesco.org/ark:/48223/pf0000381137?posInSet=7&queryId=c131b185-84ba-4e4d-8a28-94ecfdb2ffba

54 UN Secretary General, Human Rights in the Administration of Justice, A/79/296, August 2024, https://docs.un.org/en/A/79/296, highlighting, inter alia, the human rights impacts of the use of digital technologies and AI in the administration of justice.

developing a comprehensive AI strategy to guide responsible adoption and protect judicial independence. Key elements of such a strategy include:

A. Defining the Purpose and Principles for AI Use in the Judiciary

- **Clarify Strategic Objectives**: Clearly state the main goals of AI adoption – such as improving access to justice, streamlining case management, increasing efficiency, or advancing people-centered and inclusive justice or a combination of these. A focused purpose shapes decisions on which AI tools to use and how to integrate them across the Judiciary. Consider whether less resource intense alternatives to AI exist for some use cases.

- **Establish Guiding Principles**: AI systems must reflect the Judiciary's core mission and values. Foundational principles should ensure:

    - *Judicial Independence and impartiality*: Protect judicial decision-making from external influence or automation.
    - *Due Process & Fairness*: Preserve legal rights and established fair trial protections, including the right to be heard and the right to appeal. Ensure that AI is not used in cases that involve the most serious sanctions and ensure access to a human decision-maker.
    - *Human Rights*: Require respect for human rights in the development, deployment and use of AI.[55]
    - *Transparency & Explainability*: Require AI tools to be explainable, non-discriminatory, and their outcomes understandable to all stakeholders. Establish that any use of AI in judicial contexts is disclosed to all parties to the proceedings in an equitable and timely manner. Ensure that the use of AI does not compromise the right of appeal (i.e., by ensuring the parties to the proceedings have access to information about how judicial decisions were reached).
    - *Accountability*: Implement rigorous oversight, evaluation, and redress mechanisms to ensure the accuracy, safety, and fairness of any AI used, safeguard the competence of the judicial authority and protect and promote public trust in the judicial system.

55 Id., para 3, stating that the development, deployment and use of AI should be anchored in human rights.

Building on these foundations, UNESCO recommends a set of 15 principles for the development and use of AI in the Judiciary (see Fig. 1). These principles offer general guidance to ensure AI technologies are developed, acquired, and deployed in ways that respect ethics and human rights.

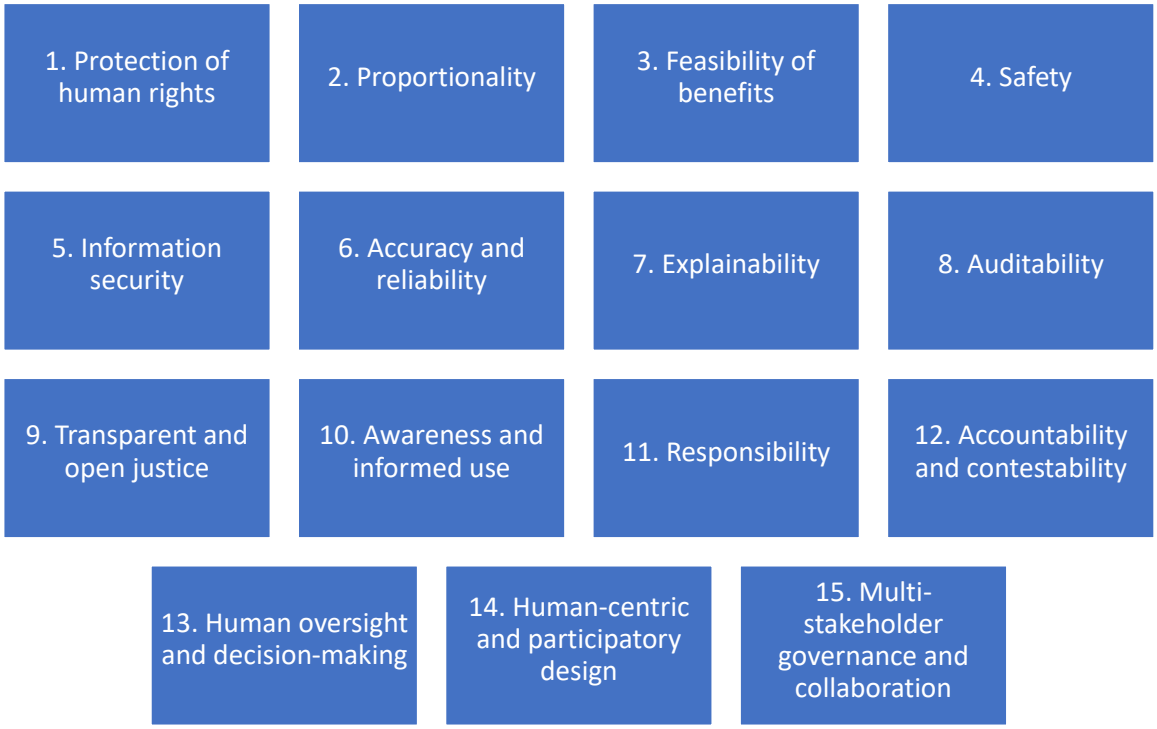

Figure 1: Principles to guide AI adoption in the judiciary

B. Establishing Foundational Elements for AI in the Judiciary

After this initial step, the judiciary must assess key foundational elements essential to developing, monitoring, and sustaining AI systems:

- Robust IT Infrastructure: Evaluate whether current technology meets requirements for accurate, fair, secure, and scalable AI deployment – such as high-speed connectivity,

computing capacity, digital court records, as well as robust data protection safeguards and built-in accuracy and safety features.[56].

- Data Management and Data Protection Practices: Review how judicial data is collected, stored, and annotated to ensure the right to privacy and non-discrimination, security, and compliance, as well as fair trial rights including the right of appeal. High-quality, well-governed data is critical for AI accuracy. Robust data protection safeguards are vital for promoting public trust, and upholding the integrity of the judicial system. UNESCO's Data Governance Toolkit[57] offers a comprehensive framework and checklist to support courts in strengthening these practices.
- Governance Structures: Assess whether existing committees or bodies for digital court transformation within the Judiciary can oversee the development, implementation, monitoring, and compliance of the AI strategy. AI should not be used in cases involving severe sanctions, vulnerable populations, or discrimination risk until robust protections and oversight are in place.
- Budgeting for Innovation: Assess the available financial resources to determine whether AI development is outsourced or built internally, and whether foundational data infrastructure should be prioritised first. Tailored safeguards and governance mechanisms are required depending on whether the AI is outsourced or built and owned by the national judicial authority.

Judiciaries may also align their AI Strategy with national legislation and AI safety and innovation strategies, to leverage broader technological synergies and expertise, and to ensure integrated, safe, and sustainable innovation.

C. Key Elements for an Effective AI Strategy in the Judiciary

56 See, OECD, AI Procurement in a Box, March 2023, https://oecd.ai/en/catalogue/tools/ai-procurement-in-a-box ; World Economic Forum, Unlocking Public Sector AI AI Procurement in a Box: AI Government Procurement Guidelines, June 2020, https://www3.weforum.org/docs/WEF_AI_Procurement_in_a_Box_AI_Government_Procurement_Guidelines_2020.pdf

57 UNESCO, Data governance toolkit: navigating data in the digital age, 2025, https://unesdoc.unesco.org/ark:/48223/pf0000394518

During the process of elaboration of the strategy, many choices will need to be made. The section below outlines some key elements for an AI Strategy in the Judiciary:

i. Build, Buy, or Both? Determining the Approach to AI Solutions

When adopting AI, Judiciaries face a strategic choice between building systems in-house or buying ready-made solutions. Custom development offers tailored features, direct control over data, and stronger alignment with legal and ethical standards, but requires considerable investment in technical expertise, maintenance, and longer project timelines. Judicial independence and impartiality could be undermined if the Judiciary is not involved in the selection of training data, or the design of the algorithm to be used in the court room.[58] In contrast, purchasing external solutions enables faster deployment and vendor support, reducing the technical burden, but may present challenges such as limited adaptability to local legal frameworks, data sovereignty risks, potential vendor lock-in, and resource inefficiency resulting in negative climate impact. Careful evaluation is essential to ensure any chosen approach upholds judicial standards, judicial independence and impartiality, transparency, the right to privacy and other human rights including non-discrimination. Open-source Digital Public Goods can help bridge the gap by providing adaptable resources for custom or hybrid models.

The UK Ministry of Justice's "AI Action Plan for Justice" outlines a multi-year strategy, developed with input from the Judiciary and legal regulators, to enhance justice delivery through AI. The plan prioritises strong foundations – leadership, governance, ethics, and secure digital infrastructure – and uses a "Scan, Pilot, Scale" model: new AI tools are assessed, rigorously piloted with oversight, and only effective solutions (like AI-driven transcription, scheduling, and case management) are scaled in courts. Supported by a Chief AI Officer, cross-departmental oversight, and systematic workforce training, the strategy is rolled out over three years with a focus on human oversight, ethics, legal compliance, and public trust.

Source: Ministry of Justice, Lord Timpson OBE, AI Action Plan for Justice, 31 July, 2025, https://www.gov.uk/government/publications/ai-action-plan-for-justice

Box 3: UK's AI Strategy for the Judiciary

ii. Prioritising High-Impact AI Applications

58 UN Secretary General, report of the Secretary General, Human Rights in the Administration of Justice, A/79/296, August 2024, paragraph 19.

AI systems can enhance a wide range of judicial tasks, but an effective strategy should focus on areas with the greatest potential benefits. By prioritising high-impact applications – such as automating case triage, streamlining document review, advancing legal research, or improving scheduling – courts can achieve quick wins and build trust in new technology – provided the accuracy and human oversight of such systems is assured. Starting with pilot projects in less sensitive areas while ensuring safety, accuracy, and efficiency helps minimise risk, while feedback from judicial staff enables ongoing refinement and smoother, broader adoption. This phased approach ensures efficient use of resources and minimises disruption to core judicial functions.

iii. Ensuring Oversight and Accountability

The Judiciary should have an oversight role and responsibility in the development, deployment and use of AI.[59] Robust oversight is vital to ensure AI tools uphold judicial integrity. Effective oversight starts with the creation of multidisciplinary judicial AI oversight committees, with gender-balanced representation and independent experts. It should be created and engaged from the project's design and relies on ongoing audits and transparent reporting to monitor bias, discrimination, privacy risks, and technical issues. Public and expert feedback helps courts address emerging challenges and offers valuable insights as to the public and professional appetite for AI adoption, while governance frameworks should be regularly updated to reflect new technologies and societal needs. Above all, oversight must safeguard human rights and due process, as outlined in UNESCO's guidelines for AI in courts.[60]

iv. Strengthening Human Capacity and Leadership for AI in the Judiciary

Building effective and responsible AI in the Judiciary requires more than technical solutions – it hinges on robust human and institutional capacity, combined with engaged and visionary leadership. Judges and court staff must be equipped not just to use, but to understand, guide and govern AI's design, development and deployment. This involves continuous training[61] on

59 Id., para. 37 and e in "Conclusions and Recommendations".

60 UNESCO, Guidelines for the Use of AI in Courts and Tribunals, 2025, https://unesdoc.unesco.org/ark:/48223/pf0000393682?posInSet=1&queryId=083af8fc-3525-4b21-8ca7-7c6274a004c6

61 UNESCO, AI and the Rule of Law: Capacity Building for Judicial Systems, https://www.unesco.org/en/artificial-intelligence/rule-law/mooc-judges ; Access to the MOOC on AI & the Rule of Law : https://www.judges.org/ai_and_law/english/

digital and AI concepts, ethical, human rights risks and legal implications, and the development of critical thinking about technology's limitations.

Recruiting and upskilling specialists – including technologists, data analysts, and digital project managers – ensures the judiciary can develop, procure, and scrutinise AI tools. This capacity is reinforced by permanent support structures, such as digital transformation units or AI steering groups, that keep courts adaptive to evolving technology and legal standards.

Success also depends on institutional knowledge sharing, open communication, and active staff engagement at all levels. Strong leadership is vital for articulating strategy, securing resources, fostering a culture of openness, and addressing concerns throughout the organisation. Recognising early adopters and involving staff in pilots encourages innovation, trust, and bottom-up learning.

France's 2025 judicial AI strategy prioritises efficiency while safeguarding ethics and judicial independence. Developed through broad consultation, it outlines ten operational priorities, including a phased rollout of a secure AI assistant for legal research, case analysis, and drafting, plus the creation of an AI observatory for oversight and a digital campus for staff training. The plan's three-stage rollout – from pilot tools in 2025 to full integration by 2027 – is backed by sustained investment.

Compliant with EU regulations and France's data protection laws, the strategy emphasises that AI is an aid, not a replacement for human judgment. By upholding transparency and accountability and investing in robust oversight and training, France's AI strategy for the Judiciary supports the responsible, human-centered adoption of AI in justice systems.

Source: Ministère de la Justice, L'IA au service de la justice : stratégie et solutions opérationnelles, June 2025, https://www.justice.gouv.fr/sites/default/files/2025-06/rapport_ia_au_service_de_la_justice_0.pdf

Box 4: France's AI Strategy for the Judiciary

v. Building New Collaborations

Successful AI integration depends on strong partnerships outside the Judiciary. Collaboration with international organisations, universities, and research centres provides essential expertise and helps uphold legal, human rights and ethical standards. Learning from the experience of other countries through platforms like the J20 can also bring fresh ideas. Technology companies offer innovation and practical tools, but these partnerships must safeguard judicial independence and impartiality, human rights and data integrity. Engagement with civil society and user groups ensures transparency, user-focused design, and public trust. Cross-sector collaboration also enables shared resources, co-developed

solutions, and joint capacity building, making AI adoption more effective and contextually relevant.

4. Judicial Independence and AI

Judicial independence and impartiality are foundational principles for the rule of law and fair trials, as established under Article 14 of the International Covenant on Civil and Political Rights, adopted by the United Nations General Assembly in 1966, and interpreted in the Human Rights Committee's General Comment No. 32 (CCPR/C/GC/32). Article 14 establishes the right of everyone to a fair and public hearing by a competent, independent and impartial tribunal established by law. The Judiciary 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 can control or direct the Judiciary is incompatible with the notion of an independent tribunal (CCPR/C/GC/32).

Brazil's Judiciary has formalised its AI strategy through the National Artificial Intelligence Committee, which develops best-practices guidelines for courts nationwide. AI tools are used to automatically classify and prioritise cases – crucial for managing Brazil's heavy backlog. Notably, São Paulo's State Court reports an 87% reduction in case processing times after adopting AI solutions. Brazil's approach blends rule-based and machine learning systems under strict human oversight, with ongoing training for judges and staff and continuous reviews to safeguard transparency and fundamental rights.

Source: National Council of Justice of Brazil, Resolution No. 615/2025, March 11, 2025 Guidelines for the Development, Use, and Governance of Artificial Intelligence Solutions within the Judiciary, English translation available at : https://rm.coe.int/resolution-6152025/1680b51b66

Box 5: Brazil's AI Strategy for the Judiciary

The UN General Assembly's 1985 Basic Principles on the Independence of the Judiciary state: "The judiciary shall decide matters before them impartially, on the basis of facts and in accordance with the law, without any restrictions, improper influences, inducements, pressures, threats or interferences, direct or indirect, from any quarter or for any reason. (…) There shall not be any inappropriate or unwarranted interference with the judicial process, nor shall judicial decisions by the courts be subject to revision."[62]

62 United Nations General Assembly, Basic Principles on the Independence of the Judiciary, September 6, 1985, endorsed by the General Assembly in its resolutions 40/32 (Seventh United Nations Congress on the Prevention of Crime and the Treatment of Offenders) and 40/146 (Human Rights in the Administration of Justice) https://www.ohchr.org/fr/instruments-mechanisms/instruments/basic-principles-independence-judiciary

Building on this, the 2008 Bangalore Principles of Judicial Conduct describe judicial independence as "a prerequisite to the rule of law and a fundamental guarantee of a fair trial. A judge shall therefore uphold and exemplify judicial independence in both its individual and institutional aspects."[63] Independence has both internal and external dimensions: internally, judges must be free from undue influence within the Judiciary itself; externally, they must be shielded from pressures by the Executive, Legislature, parties to a case, the public, or any relationships that could affect the perception of their impartiality.

The use of artificial intelligence in the Judiciary – especially generative AI tools – creates new challenges to both internal and external judicial independence. These technologies require heightened vigilance and refined standards, as they can introduce novel forms of error, influence, or discrimination and complicate traditional safeguards including fair trial rights and human rights. Courts and judges must continue to adapt to ensure that the essential principle of judicial independence is upheld in the face of technological change.

A. AI as a strength or a threat to judicial independence

Artificial intelligence has the potential to both enhance and challenge judicial independence, depending on how it is implemented and governed. When thoughtfully applied, AI can support judges by providing access to comprehensive legal data, improving analytical capabilities, and automating routine tasks. These benefits can boost efficiency and consistency, freeing judges to focus more on independent legal reasoning and fair decision-making.

However, there are also significant risks. AI can introduce new threats to independence both directly – through the design and limitations of algorithms[64] – and indirectly, due to practical

63 Bangalore Principles of Judicial Conduct, 2002, value 1, p.8, https://www.unodc.org/documents/ji/training/bangaloreprinciples.pdf ; see also, European Commission for Democracy through Law (Venice Commission), Report on the Independence of the Judicial System. Part I: The Independence of Judges, Study No. 494 / 2008 CDL-AD(2010)004, March 2010 ; See also art 26 of African Charter on Human and Peoples' Rights ; Report of the Special Rapporteur on the independence of judges and lawyers, Diego García-Sayán, submitted pursuant to Human Rights Council resolution 35/11, A/74/176, July 2019, https://docs.un.org/en/A/74/176

64 UN Secretary General, report of the Secretary General, Human Rights in the Administration of Justice, A/79/296, August 2024, paragraph 19

realities in courts. For example, the development of data tools by the Executive 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.[65] Judges, recognised for their professionalism and critical thinking, face daily pressures such as heavy caseloads and limited time. These conditions can make AI tools appealing for efficiency but also increase susceptibility to automation bias: the tendency to over-rely on AI-generated outputs, sometimes at the expense of independent judgment. This risk is heightened if systems lack transparency or contain errors or systemic biases, potentially leading to discrimination, unfair outcomes and diminished institutional trust.

It is important to recognise that discussing risks to judicial independence does not diminish judges' expertise or integrity but rather aims to ensure that safeguards are in place so that new technologies reinforce – rather than erode – the bedrock principles of impartiality and the rule of law.

B. Motivation of court decision, right to appeal, and black box problem

A fair trial depends on transparent judicial reasoning. Judges are duty-bound to provide clear, well-motivated decisions grounded in factual and legal analysis, as this transparency enables meaningful appeals – where not only the outcome but the underlying reasoning can be challenged. A trial can therefore only be fair if the judge's reasoning is transparent. As Bentham observed, "Publicity is the very soul of justice. (…) Where there is no publicity, there is no justice." [66]

With the growing use of AI and algorithmic tools in courts, a new challenge – known as the "black box" problem – has emerged. The complex and often opaque computational processes of many AI systems can make it difficult for judges to interrogate, verify, or fully understand the outputs these tools provide. This opacity risks judicial independence in several ways. Judges may become overly reliant on algorithmic recommendations or AI-generated content,

65 Id., paragraph 37

66 *The Works of Jeremy Bentham*, published under the Superintendence of his Executor, John Bowring (Edinburgh: William Tait, 1838-1843), 11 vols, Vol. 4, p.316

subconsciously influenced by outputs they cannot explain, thereby ceding crucial aspects of their decision-making authority to automated systems.

Further complicating matters, generative AI tools, while helpful in synthesizing research, drafting documents, and analysing evidence, can amplify automation bias. Judges may be tempted to endorse AI-driven synthetic text production without rigorous scrutiny, risking decisions based on inaccurate, misleading, or even fabricated information ("hallucinations"). Additionally, generative AI models have demonstrated a tendency toward sycophancy – and confirming the assumptions implied in prompts to "please" the user. While AI labs seek to address this problem, the outputs of generative AI tools should be reviewed with a high degree of caution. Where judicial decisions are informed by AI, there is a strong risk that judicial expertise and legal reasoning is sidelined and motivation of decisions undermined, jeopardising the fairness and credibility of the hearing and the judicial outcome. Most notably, fair trial rights could be undermined: when defendants are unaware that AI systems were used to make a decision affecting 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.[67]

Ultimately, while AI use has the potential to enhance efficiency and expand access to legal information, it also demands heightened vigilance. To uphold justice and to maintain public trust, judges must ensure their decisions remain independently reasoned and fully explainable, resisting undue reliance on opaque and, at times, unreliable technologies.

C. Ensuring Judicial Control over AI Systems

In the judicial context, who controls the AI system, its data, and underlying algorithms shapes how information is generated for use in court. This is not simply a technical issue but rather a more political question about who selects, curates, and determines the information that guides judicial reasoning. The risk of improper influence is particularly high when control is exerted by non-judicial actors with an interest in deciding judicial outcomes, including governments or

67 UN Secretary General, report of the Secretary General, Human Rights in the Administration of Justice, A/79/296, August 2024, paragraph 17

corporations. AI models are often complex and often opaque, relying on neural networks with billions of parameters to produce outputs that even experts struggle to fully explain.

When judges use AI tools for drafting or analysis, the content produced only becomes an official decision once endorsed by the judge. However, there is a risk that reliance on AI may subtly shape or constrain a judge's reasoning, embedding judicial thinking within the logic and limitations set by the technology and its developers. In some cases, judges may unconsciously adapt their approach to mimic the decision patterns of AI models, potentially diminishing their intellectual and judicial independence.

While some argue AI can expand judicial insight by surfacing overlooked information and compensating for human limitations, real-world experience will ultimately determine whether this empowerment outweighs the risks. To safeguard judicial independence, it is critical that AI systems and their interfaces are designed to keep judges firmly in control – supporting, but never supplanting independent judicial thought and decision-making. For this reason, the Judiciary should have an oversight role and responsibility in the development, deployment and use of AI.[68]

D. Independence from Peers and Institutional Dynamics

Generative AI's ability to produce standardised legal reasoning could unintentionally promote conformity among judges, diminishing the intellectual diversity and nuanced analysis that are vital for justice. As AI tools become embedded in court operations, judges may feel subtle pressure – whether from colleagues or institutional expectations – to rely on these systems, which can constrain individual discretion. Over time, widespread use of AI may lead to a judicial culture where decision-making styles increasingly reflect algorithmic norms rather than independent, case-specific judgment, raising important concerns about maintaining judicial independence from both peer influence and internal institutional pressures. This also risks impacting human empathy and legal discretion, that are essential for any judge, particularly in criminal justice, of which AI systems are not capable.[69]

68 UNESCO Guidelines for the Use of AI in Courts and Tribunals, May 2025, p.15, 17.
69 UN Secretary General Report on the Administration of Justice, A/79/296, para. 21.

E. Independence from External Pressures: Public, Media, and AI Providers

The adoption of generative AI in the Judiciary brings increased scrutiny from the public and media, both of which play a significant role in shaping perceptions of judicial legitimacy. If AI-generated decisions or reasoning lack transparency, are inaccurate or incorporate hallucinations, public trust in the courts may erode, leaving the Judiciary vulnerable to criticism or political pressure. Additionally, the ability of litigants to use AI tools to analyse patterns in judges' past rulings can encourage forum shopping or strategic litigation, subtly influencing judicial behaviour.

Perhaps most critically, reliance on AI systems provided by private companies introduces the risk that technology firms – through their control over algorithm design, data management, or system updates – could exert undue influence over judicial processes. This dependence on external commercial providers raises important questions about maintaining true judicial autonomy and safeguarding the integrity of legal decision-making within a framework whereby the State retains responsibility for the delivery of essential public services.

F. Further reflection

While the intersection of judicial independence and artificial intelligence is still a relatively new and evolving topic, it is the subject of ongoing debate among courts, policymakers, and experts worldwide. Many of the risks and opportunities are not yet fully understood, and practical safeguards and best practices are still emerging. In this context, we propose the following key questions for further discussion among J20 members to support critical reflection and informed decision-making as AI adoption in the Judiciary continues to unfold:

- What is the value proposition of AI for the Judiciary and what are the key elements for developing an AI strategy for the Judiciary? How can States' capacity be enhanced to develop tailored AI solutions for the Judiciary?
- How will States ensure responsible procurement and full lifecycle control – including updates, retraining, and contractual termination – when contracting private AI providers?

- How can courts ensure that AI systems support, rather than undermine, the autonomy and independent judgment of judges including in the implementation of human rights such as fair trial rights, and rights to liberty and security – especially given the risks of automation bias and opaque ("black box") algorithms?
- What safeguards should be in place to guarantee that AI-generated content or recommendations do not replace judicial reasoning, and that judges remain fully accountable for their decisions?
- What mechanisms are necessary to protect the Judiciary from external influence by AI providers or institutional pressures to conform to AI-generated norms, while upholding both individual and institutional independence? What are the implications of procurement of AI solutions for the Judiciary developed by the private sector?
- How can courts maintain transparency and explainability in the use of AI, so that parties and the public clearly understand when and how AI influences judicial processes – and can challenge decisions if needed?
- What mandatory disclosures of AI usage should courts implement per trial?
- What minimum oversight and audit mechanisms should be legally required for judicial AI systems?

5. Conclusion

As courts worldwide face opportunities and risks brought about by artificial intelligence, developing a comprehensive and principled AI strategy is vital for the Judiciary's continued effectiveness and legitimacy. Clearly defining the intended purposes and guiding principles for AI integration ensures that technological advancement is consistent with the fundamental values of justice, transparency, and public trust, and compliant with human rights international standards. Building strong foundational elements – such as modern, reliable and secure IT infrastructure and digital court records – creates the necessary conditions for AI adoption that is both responsible and sustainable. Considering resource efficiency of data infrastructure and AI models ensures the compatibility between progress and climate protection.

In addition, careful assessment of current capabilities and strategic investment in technology will allow judicial institutions to harness the benefits of AI while maintaining the highest standards of fairness and respect for human rights. The process demands ongoing vigilance to ensure that digital transformation enhances, rather than undermines, the rule of law, human

rights and the dignity of all those who engage with the justice system. By approaching AI adoption thoughtfully and deliberately, the Judiciary strengthens its ability to deliver justice in an increasingly digital and complex world.

To safeguard the rule of law and judicial independence, courts must ensure that technology supports, rather than interferes with, impartial decision-making. The responsible application of AI must be carefully balanced to preserve the integrity and independence of the Judiciary, ensuring that algorithmic tools do not compromise established legal principles and human rights standards or the public's confidence in unbiased and non-discriminatory adjudication. Continuous scrutiny and reflection are necessary to maintain this independence, especially as new forms of decision support technology emerge.

UNESCO supports J20 as a knowledge partner and prepared this issue brief to inform J20 members on important issues related to AI in the Judiciary.

Document authored by:

Prateek Sibal, Programme Specialist, Digital Policies and Digital Transformation Section, UNESCO and Dr. Kamel El Hilali, Individual Specialist, AI & the Rule of Law, UNESCO.

Acknowledgements:

In the development of this issue brief, we received helpful input and suggestions from Dr. Gomolemo Moshoeu, South African Judicial Education Institute (SAJEI), Margaret L. Satterthwaite, UN Special Rapporteur on the Independence of Judges and Lawyers, Professor of Law, New York University School of Law, Katarina Sydow, External Legal Advisor to the Special Rapporteur on the independence of judges and lawyers, Adjunct Professor, New York University School of Law, Kate Fox, OHCHR, Wendy O Brian, UNODC, Guilherme Canela, UNESCO, Cedric Wachholz, UNESCO and Virginia Antonelli, UNESCO.

About UNESCO's Judges Initiative:

Operating in over 160 countries, this innovative program offers comprehensive and practical training tools to members of the judiciary, in order to strengthen knowledge and capacities on regional and international standards on freedom of expression, access to information, the safety of journalists and AI and the Rule of Law. By providing judicial actors with a better understanding of their role in the protection of freedom of expression, UNESCO aims to foster the rule of law and support justice systems to become more aware on how to protect journalists against attacks and prosecute the crimes against them.

Looking back to the last 12 years, the Judges' Initiative has made significant progress and had real positive impact on an international scale:

- Over 36,000 judicial actors and civil society representatives trained from 160 countries since its inception in 2013.

- 11 Memorandum of Understanding established with regional human rights courts and judicial institutions.
- 10 freely accessible Massive Open Online Courses (MOOCs) offered to judicial actors.
- 12 resources and guidelines published for judicial actors and training institutes in multiple national and local languages.
- A global database of over 2,700 judicial case laws supported.

More about UNESCO's Judges Initiative at: https://www.unesco.org/en/articles/10-years-unescos-judges-initiative
More about UNESCO's AI and the Rule of Law programme at: https://www.unesco.org/en/artificial-intelligence/rule-law

Key UNESCO resources on AI and the Judiciary:

- Global toolkit on AI and the rule of law for the judiciary - UNESCO Digital Library
- Guidelines for the Use of AI Systems in Courts and Tribunals - UNESCO Digital Library
- Global Judges' Initiative: survey on the use of AI systems by judicial operators
- UNESCO Network of Experts on AI and the Rule of Law

Additional References

United Nations

- Report of the Secretary General, Human rights in the administration of justice A/79/296. This report highlights the human rights challenges and good practices of the application of digital technologies and artificial intelligence in the administration of justice
- The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights, A/HRC/48/31
- Reimagining justice: confronting contemporary challenges to the independence of judges and lawyers Report of the Special Rapporteur on the independence of judges and lawyers, Margaret Satterthwaite, A/HRC/53/31

- A/RES/78/265 Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development
- A/RES/78/311 Enhancing international cooperation on capacity-building of artificial intelligence

European Union

- European Commission for the Efficiency of Justice (CEPEJ), Report on the First Use of the Self-Assessment Tool for AI Systems in the Judicial Field: General Aspects, May 22, 2025, https://rm.coe.int/cepej-gt-qual-2025-6-rev2-rapport-sur-l-utilisation-de-l-outil-d-auto-/1680b6d03c

Council of Europe

- CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment, https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment
- CEPEJ, Working Group on Cyberjustice and Artificial Intelligence, Advisory Board on Artificial Intelligence, 1st AIAB Report on the use of Artificial Intelligence (AI) in the Judiciary based on the information contained in the Resource Centre on Cyberjustice and AI, 28 February 2025, Https://Rm.Coe.Int/Cepej-Aiab-2024-4rev5-En-First-Aiab-Report-2788-0938-9324-V-1/1680b49def

Australia

- Justice Jane Needham, Federal Court of Australia, AI and the Courts in 2025. Where are we, and how did we get here?, 27 June 2025 https://www.fedcourt.gov.au/digital-law-library/judges-speeches/justice-needham/needham-j-20250627

Brazil

- National Council of Justice of Brazil, Resolution No. 615/2025, March 11, 2025, Guidelines for the Development, Use, and Governance of Artificial Intelligence Solutions within the Judiciary, English translation available at: https://rm.coe.int/resolution-6152025/1680b51b66

Canada

- Guidelines for the Use of Artificial Intelligence in Canadian Courts, September 2024, https://cjc-ccm.ca/sites/default/files/documents/2024/AI%20Guidelines%20-%20FINAL%20-%202024-09%20-%20EN.pdf

Colombia

- Guidelines for the respectful, responsible, safe and ethical use and exploitation of artificial intelligence in the Judicial Branch, Higher Council of the Judiciary of Colombia, Agreement PCSJA24-12243, of 16 December 2024, https://actosadministrativos.ramajudicial.gov.co/web/Acto%20Administrativo/Default.aspx?ID=19280

France

- CNIL, AI: The CNIL finalises its recommendations on the development of artificial intelligence systems and announces its upcoming work, 22 July 2025, https://www.cnil.fr/en/ai-cnil-finalises-its-recommendations-development-artificial-intelligence-systems
- Secrétariat général de la défense et de la sécurité nationale, Challenges and opportunities of Artificial Intelligence in the fight against information manipulation, February 7, 2025, https://www.sgdsn.gouv.fr/files/files/Publications/20250207_NP_SGDSN_VIGINUM_Rapport%20menace%20informationnelle%20IA_EN_0.pdf
- Defenseur des Droits, Algorithms, AI systems and public services: what rights do users have? Critical Considerations and Recommendations, 2024 https://www.defenseurdesdroits.fr/sites/default/files/2025-01/DDD_rapport_algorithmes-systemes-d-IA-et-services-publics_EN_2024_20250109.pdf

India

- The High Court of Kerala AI Policy, July 19, 2025, https://nationalcenterforstatecourts.app.box.com/s/k0q208g72a2m8jpzv08mwxx8azesfixa

New Zealand, Aotearoa

- Guidelines for Use of Generative Artificial Intelligence in Courts and Tribunals, December 7, 2023, https://www.courtsofnz.govt.nz/assets/6-Going-to-Court/practice-directions/practice-guidelines/all-benches/20231207-GenAI-Guidelines-Judicial.pdf

The United Kingdom

- Policy paper AI action plan for justice, July 31, 2025, https://www.gov.uk/government/publications/ai-action-plan-for-justice/ai-action-plan-for-justice

The United States

Nationale Center for State Courts

- Conference of State Court Administrators, Generative AI & the future of the courts. Responsibilities and Possibilities, August 2024, https://www.ncsc.org/resources-courts/generative-ai-future-courts
- Leveraging AI to reshape the future of courts, https://www.ncsc.org/resources-courts/leveraging-ai-reshape-future-courts
- Mapping of AI Efforts (statutes and proposed legislation, caselaw and decisions, attorneys/judicial codes of conduct, guidelines and policies, AI rapid response team, Task forces/committees, projects, rules, videos, webinars,) used in State courts: https://www.ncsctableauserver.org/t/Communications/views/AIRRT/AIResources?%3Aembed=y&%3AisGuestRedirectFromVizportal=y

J20
SOUTH AFRICA 2025

Solidarity
Equality
Sustainability

BRIEFING PAPER: Day 2 Plenary Session 4

Combating Cybercrime: Strengthening Cross-Border Judicial Cooperation

#J20SouthAfrica | #ReKaofela | www.j20.judiciary.org.za

Justice in a time of change: Independence, Innovation and Co-operation

G20
SOUTH AFRICA 2025

unesco

juta

South Africa
Inspiring new ways
www.southafrica.net

BRIEFING PAPER: Day 2 Plenary Session 4

Combating Cybercrime: Strengthening Cross-Border Judicial Cooperation

Contents

1. Background

With globalization and the pursuit of development, countries have become more interdependent and connected. The contemporary world has introduced changes in social interactions, trade, and politics, evidenced by a significant in cross-border activities. This is a time when most persons, both natural and juristic, have transnational links and carry out activities beyond their host states or countries of origin.

As a result, there are 'interconnections between legal systems and actors within these systems'.[70] Consequently, approaches to law and justice have had to change; judiciaries from across the world are forced to adapt and cooperate in ensuring the efficient and effective administration of justice to address the transnational legal issues, including cybercrime. Recognising that cybercrimes transcend national borders, the aim of this session is to facilitate discussions and exchanges that transcend geopolitical boundaries and will encourage cooperation and synergy among Judiciaries.

International judicial cooperation takes various forms and can be defined in a myriad of ways. The general understanding behind this notion is that it refers to the ability of states to work together in the administration of justice in matters with a cross-jurisdictional nature. Judicial cooperation can manifest in various ways, both formal and informal, and can apply to matters of a criminal and civil nature, but for purposes of this dialogue, emphasis will be on cybercrime as a novel and expanding area in judicial focus.

The significance of judicial cooperation in combating cybercrimes lies in the allowances it makes for information sharing and knowledge dissemination. Judicial cooperation ensures that there is efficiency in cybercrime prosecutions as it facilitates the swift exchange and access to evidence, arrests of accused persons, and coordination in simultaneous legal actions. Additionally, united efforts to protect digital ecosystems promote trust in global digital infrastructure.

2. Objectives

The aim of the session on international judicial cooperation is to discuss: topical transnational issues, and the prompted call for increased judicial cooperation, their impact on the Judiciary

70 E Mak, N Graaf and E Jackson "The framework for Judicial Cooperation in the European Union: Unpacking the Ethical, Legal and Institutional Dimensions of Judicial Culture" (2018) 34(1) *Utrecht Journal of International and European Law* 29.

and the role of the Judiciary in addressing these matters; the changing legal landscape and challenges posed for the superior courts and constitutional courts of G20 members. Along with a discussion on potential strategies on how judicial cooperation can be used to: combat transnational crimes (particularly cybercrime) and ensure the administration of justice while addressing wider global issues.

Furthermore, the session offers an opportunity for discussion on the challenges to judicial cooperation in addressing cybercrime, its limitations, and the formulation of solutions to foster judicial cooperation – with or without the existence of formal international instruments –. Furthermore, the session aims to facilitate dialogues on how a shared judicial culture between judges from G20 states can serve the achievement of law enforcement and the protection of human rights, as well as cooperation between the Judiciaries. Overall, it is hoped that we will gain insight into how the different Judiciaries have approached cybercrime as an emerging threat by facilitating the exchange of best practices, experiences, and legal innovations or solutions to this transnational issue.

3. Transborder Judicial Cooperation

3.1 Transborder Judicial Cooperation in Addressing Broader Global Issues

Generally, Judicial cooperation is vital in dealing with broader societal issues. This ensures the sustainability of justice in times when legal issues change shape and form. With the institutional ascent of Judiciaries in recent years, the courts have had to grapple with political, social, and public policy issues that affect the justiciable fundamental rights (particularly social and economic rights), which are incorporated into our constitutions. This "judicialization" of matters and involvement of the judiciary in realising these rights, has meant that the Judiciary has gradually had to make determinations which directly influence policymaking, human rights protection, and the resolution of political disputes.[71] More topically, judicial cooperation has become necessary in addressing cybercrime as a new and ever-expanding global dilemma.

3.2 Judicial Cooperation in combatting Cybercrime

Generally, the premise for judicial cooperation in criminal matters is based on the mutual recognition that it is in the interest of the global community that those who have committed crimes, be it individual persons or groups, be prosecuted.[72] At a time when criminals have

71 D L Scribner “The Judicialization of (Separation of Powers) Politics: Lessons from Chile” (2010) vol 2(3) *Journal of Politics in Latin America* 2010 71-72.

72 G O Antai “Methods of Judicial Cooperation and the Procedure for Enforcement Under International Law; Identifying the Nexus between Theory and Practice” (2024) vol 4(3) 80.

exploited the globalised economy, mainly, its free markets, open borders, and technological advances, the sophisticated and rapidly evolving nature of transnational organized crimes necessitates a coordinated global response from G20 states and their judiciaries.

Purwawijaya *et al*[73] note the impact of evolving tactics in cybercrime and how 'cybercriminals continue to develop methods and tools to breach security systems. With increasingly sophisticated technology, they can easily find loopholes in cybersecurity and exploit them for personal gain or other malicious purposes'[74]and this has significant implications for our society thus coordinated and effective measures are essential to mitigate the impact of cybercrime and ensure the stability and functionality of the digital world.

Therefore, the aim of this section is to consider the types of cybercrimes, the legislative framework regulating this area, the challenges posed, judicial responses and to discuss how justice mechanisms can be improved in strengthening transborder cooperation efforts.

3.3 Addressing Cybercrimes

The rapidly growing digitalized space and use of electronic communication systems have presented novel forms of crimes, particularly in the fields of cybersecurity and cyberspace.[75] As technology has evolved, so have the methods utilized by criminal actors and there has been an increase in illegal activities committed through digital means. This has created a need for judiciaries to adapt in order to meet emerging threats that result from new technologies.[76] Cybercrime covers a wide range of offences, which include but are not limited to: the unlawful access to information, interception of data, the use of software or hardware to use or possess programs which facilitate the commission of cybercrimes, unlawful interference with data or computer programs, data storage or computer systems, cyber fraud, cyber-terrorism, cyber-stalking, child exploitation,[77] Identity theft, forgery and uttering, cyber extortion, cyber espionage, theft of incorporeal property, malicious communication.

---

73 E Purwawijaya, D Syahputra, A Rambe, J Nababan, "The Significant Rise In Cybercrime Can Be Attributed To Vulnerabilities In Cybersecurity." (2024).*Jurnal Minfo Polgan* 13(1) 113.

74 *Ibid* 112.

75 G Goosen 'Cybercrime' *The South African Judicial Education Institute Book* (2025) 73.

76 M Sridevi 'Decoding the Cyber Legal Landscape: Judicial Strategies in cybersecurity and cyber-crime proceedings'

77 Which includes the creation, sharing and/or distributing of child pornography or the use of digital technologies to exploit or abuse children online.

From a regulatory perspective, attempts have been made on international and domestic fronts to adopt and implement laws that will address challenges that arise from the cyber legal landscape.

3.4 The international legal framework regulating cybercrimes

International regulation initiatives include the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, [78] and the Convention on Cybercrime, commonly known as the Budapest Convention, which is considered the principal international treaty dealing with cybercrime. [79] This instrument has been significant in its ability to provide a framework and measures for member and signatory states to adopt legislation at a national level. According to Goosen, it 'criminalises certain conduct and fosters international cooperation while recognizing and protecting the right to use and develop digital systems'.[80] Moreover, the Convention has been instrumental in facilitating international cooperation, particularly through its requirement for the establishment of a 'network of Points of Contact in each signatory state which would operate on a 24-hour, seven-day-week basis to allow for immediate and expedited mutual assistance in investigations'.[81] Flowing from this, individual states have instituted domestic legislative processes and implemented measures to deal with cybercrimes.[82]

3.5 Challenges in addressing cybercrime matters

Despite the existence of domestic regulatory frameworks and national strategies in addressing cybercrime, state efforts cannot occur in isolation. There is still much room for state members to implement the Budapest Convention and harmonise their fragmented enforcement efforts. Other challenges posed by cybercrime, relate to issues around the determination of jurisdiction and the difficulties in effectively prosecuting offenders (due to the anonymity of actors especially in the dark net and crypto-currency use), the lack of harmonisation in legal frameworks, procedures and definitions of crimes and inefficient mutual legal assistance (as

78 This Convention was adopted by the Council of Europe in 1980
79 Officially known as the Convention on Cybercrimes, which came into effect in July 2004.
80 G Goosen 'Cybercrime' *The South African Judicial Education Institute Book* (2025) 73.
81 *Ibid*.
82 For instance, the Republic of South Africa which still has to enact the Cyber Cybercrimes Act, has enacted other related legislation such as the Electronic Communications Act 25 of 2002, the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, the Protection of Personal Information Act 4 of 2013, and the International Co-operation in Criminal Matters Act 75 of 1996 which regulates requests received for assistance in the investigation or prosecution of criminal offences by foreign states

current processes have been critiqued for being too slow for real time investigations and the collection of evidence from foreign states has been described as difficult). [83]

As a result of these challenges, the fight against cybercrime requires concerted efforts between governments, law enforcement agencies, cybersecurity experts and the various Judiciaries. This can take place through bilateral and multilateral agreements that allow for mutual legal assistance,[84] and extraditions and the transfer of prisoners from one country to another in cyber-crime offences. For instance, initiatives that facilitate the provision of evidence and the execution of sentences in criminal cases and confiscation and transfer of proceeds of crimes to foreign states come to mind.[85] Judicial cooperation also entails the exchange of documents and judgments between nations, the provision of legal assistance, and the obtaining of evidence from different members.[86] According to Antai, this cooperation occurs when 'one state's competent authority requests assistance from another' in order to carry out specific tasks when dealing with cross-border situations.[87]

Given the backdrop of the significance of judicial cooperation in addressing cybercrimes, the next question for purposes of this dialogue is how we can foster cooperation between our judiciaries, and what are the practical steps to be taken to strengthen judicial cooperation going forward.

4. A shared judicial culture between J20 judiciaries

From a normative perspective, establishing a shared "judicial culture" is important for international judicial cooperation. It would serve the achievement of legal unity in conflict resolution, law enforcement and the protection of human rights, as well as the cooperation between judges in G20 states.[88]

"Judicial culture," according to Bell, refers to the 'features that shape the way in which the work of a judge is performed and valued within a particular legal system'.[89] This includes the

83 A Bolt "Practical problems in mutual assistance in criminal matters. Commonwealth Law Bulletin" (1993) 19(4), 1911–1916. https://doi.org/10.1080/03050718.1993.9986336

84 'South Africa has extradition agreements with Botswana, Lesotho, Malawi, Swaziland, USA, Canada, Australia, Israel, Egypt, Algeria, Nigeria, China and India'. Mujuzi 'The South African International Cooperation in Criminal Matters Act and the issue of evidence' 2015 *De Jure* 351-387.

85 For instance, South Africa has enacted the International Cooperation in Criminal Matters Act (ICCMA) Act 75 of 1996, see also Regulations GNR 1729 of 1997-12-19, GG No 18556.

86 Antai (note 3 above) 81.

87 Antai (note 3 above) 80.

88 Mak et al (note 1 above) 24.

89 Mak et al (note 1 above) 27.

actual task of judging and the organization of the judiciary itself as aspects of judicial functioning.

A shared judicial culture is possible through states' alignment of their interpretations of legal concepts and working methods. With the ever-changing criminal landscape and nature of cybercrime, knowledge exchange is required to enable judiciaries to understand and effectively respond to the complexities of advancing cybercrime networks or cybercrime ecosystems.[90] Through formal and informal avenues, Judiciaries can draw from each other, including knowledge exchange sessions, peer-to-peer learning, networking and continuous dialogues within the J20 group.

Judicial cooperation is not a new concept and has been demonstrated in the courts' ongoing ability to draw from foreign judgments, legislation and academic literature.[91] Initiatives for the judiciary to cooperate in the fight against cybercrime will ensure that those guilty of committing crimes are prosecuted in terms of the law, and that no country serves as a safe haven or refuge for criminals.[92]

The proposed shared culture is to be founded on shared principles and safeguards, namely, that all judicial coordination must be grounded in legal authority and the rule of law. Secondly, the protection of human rights must be an integral component of international cooperation. Judiciaries need to ensure that fundamental rights such as freedom of expression and privacy are observed and that due process is followed.

Thirdly, reciprocity and mutual trust are essential;[93] there must be a shared commitment by participating states to transparency, accountability, and fair legal standards. Lastly, there needs to be allowances for both public and private cooperation within strict boundaries. Judiciaries will need to leverage the knowledge, expertise, and, where applicable, the cutting-edge technologies of the private, public, and civil society sectors to ensure their readiness to deal with cybercrimes.

It is worth noting that judicial cooperation, especially when dealing with diverse judiciaries, requires a convergence of laws and methods.[94] This is because judiciaries may have differences in views on their judicial function and existing practices when judging in different

90 S Broadhead "The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments" *Computer Law & Security Review* (2018) 34(6) 1182.
91 Mak *et al* (note 1 above) 26.
92 Antai (note 2 above) 80.
93 Mak et al (note 1 above) 39.
94 Mak *et a*l (note 1 above) 26.

jurisdictions. Moreover, the context within which judging occurs varies greatly from one state to another, and as Mak *et al* note, this could influence judges' work and their shaping of domestic laws.[95] Therefore, when considering how to establish a shared culture, judges have to contemplate how they can achieve uniformity and consistency in how they apply the law and legal principles in light of the different contexts from which they perform their functions.

It is acknowledged that it might be easier to achieve collaboration between judiciaries from countries with shared backgrounds and/or similar legal systems, whereas this might be challenging for judiciaries that differ greatly and therefore proposed methods or strategies need to accommodate these nuances.

5. Proposed recommendations

Considering that cybercrime knows no boundaries and criminal acts can be committed in multiple jurisdictions, collaboration and assistance between states is important. Historically, cooperation among sovereign states in the investigation and prosecution of crimes, has been grounded in established international treaty relations and guided by the principle of comity,[96] and in strengthening judicial cooperation in combating cybercrime specifically, the following recommendations are proposed:

5.1. A Reform of Mutual Legal Assistance

As aforementioned, current mutual legal assistance procedures have been critiqued for slowing down real-time investigations in cyber-crime matters.[97] Traditional judicial cooperation methods have also been seen as being too slow for timely cross-border access to electronic evidence,[98] other contributing challenges include legal fragmentation, issues around disproportionate expense of resources and inadequate means of transmission.[99] This points to the need for improved information and intelligence sharing and efficient transnational communication.

Bearing in mind that ‘most cybercrimes are transnational in nature with extra-territorial jurisdiction’, the localization of data would aid in mitigating challenges that make it difficult to

95 Mak *et al* (note 1 above) 26.
96 E d’Alterio "From judicial comity to legal comity: A judicial solution to global disorder?" (2011) *International journal of constitutional law* 9(2) 394-424 at 399.
97 European Commission, Directorate-General for Justice and Consumers “European Commission Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters” (2018) 17/04 9 at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018SC0118 *at* 5.
98 *Ibid* 240.
99 *Ibid* 128

collect evidence from foreign territories.[100] J20 members need to consider how they can align their communication channels and processes to allow for rapid transnational responses and easier cross-border access to electronic evidence when tackling cybercrimes. Secure communication platforms need to be established for real-time judicial coordination.

5.2. Innovative judicial cooperation

Additionally, there needs to be innovations in cross-border access to digital evidence. States need to consider developing shared protocols for lawful cross-border access, and foster cooperation with both public and private actors.

The role of public-private partnerships cannot be understated; cooperation between industry stakeholders makes information sharing easier and allows for efficient counter efforts. Thus, the judiciary needs to leverage the resources and expertise of both the private and public sectors in combating cybercrimes, particularly those involved in providing digital platforms and cloud services, while still maintaining safeguards for privacy and due process.

5.3. Harmonisation of legal systems

Moreover, there needs to be aligned extradition frameworks that will ensure that cybercrime is recognized and dealt with as an extraditable offense across jurisdictions. Judiciaries need to develop rules that can serve as a model for the reception of digital evidence by the different courts to ensure consistency in their approaches.

5.4. Capacitation of the Judiciary

Furthermore, initiatives aimed at building the capacity of the Judiciary are required. This involves ensuring that judges are technologically adept to handle cyber offence cases. This includes the ongoing development of judicial education programmes and curricula which focus on cybercrimes and electronic evidence handling, to ensure that cybercrime matters are handled with the necessary expertise and understanding of technical concepts, keeping the judiciary abreast with the advent of new technologies.

---

100 MK Kannojia “Analysis of cyber-crime and cybersecurity in India” (2023) *CyberCrime & Cyber Securities in India* 10.

There is also room for exploring opportunities for benchmarking, judicial secondments and exchanges on a more frequent basis, even outside this annual summit.

Judges, as 'linchpins between their domestic legal order and the international legal order',[101] play a significant role in aligning domestic practices with the agreed international standard in handling cybercrime-related offences.

As a result of the issues discussed above, it is necessary to reflect on how judiciaries, as pivotal agents in safeguarding fundamental rights and justice, can collaborate to address transnational legal issues in the 21st century. To this end, the following questions are proposed for discussion:

6. Reflection Questions:

a. What role can the judiciary play in combating cross-border crimes, considering the hindrances to prosecuting those involved, and how these hindrances can be overcome?
b. How can legal definitions and procedures be harmonized across the J20 countries?
c. What safeguards are needed to ensure judicial cooperation does not lead to human rights abuses or unjust surveillance?
    - *How can a balance be struck between considerations supporting cyber sovereignty and freedom, versus the need for international cooperation and the sharing of data?*
d. How can the courts make access to actual remedies possible ensuring the substantive realization of human rights?

e. Is there room for judicial activism in addressing cybercrimes and ensuring inclusivity in cyber security, using a human rights approach when adjudicating?
    - *Considerations relate to dealing with systemic gaps and hurdles preventing the most vulnerable groups from accessing justice, safeguards to women's rights and dignity and shielding children from online crimes.*

f. Is a shared normative basis for judicial functioning between the judiciaries in the J20 possible?
    - *What would a global judicial culture entail, and which values would inform it? How do judiciaries converge practices where their legal systems differ greatly?*

101 Mak *et al* (note 1 above) 26.

g. How can judiciaries embark on a concerted effort to cooperate where there is no agreement in place for such cooperation between states? And how can they address transnational issues that are not governed by statute or have formal enforcement mechanisms?

h. What does international and regional cooperation entail practically?

i. What steps can be taken to ensure knowledge sharing through training and seminars, mostly online but also in person where time and budgets permit?

j. Is there scope for expanding participation of nation states through the Budapest Convention?