CENTRE DE FORMATION JUDICIAIRE DU SÉNÉGAL

Intelligence artificielle et pratique judiciaire :

LA PREUVE NUMÉRIQUE

Gora Ngom | BRIO Academy | 14 avril 2026

L'ACCROCHE

Février 2024 — Hong Kong. Un cadre financier effectue un virement de **25,5 millions de dollars** après une visioconférence avec ses supérieurs. Tous étaient des deepfakes générés par intelligence artificielle. Aucun des participants n'existait réellement.

interview du PDG de ARUP

Indiscernables

À l'œil et à l'oreille,
les faux étaient parfaits

Accessibles

Les outils sont disponibles
sans expertise particulière

Déjà dans les dossiers

Le phénomène touche
les juridictions du monde entier

Si la technologie peut tromper un professionnel aguerri, quelles précautions le juge doit-il prendre face à une preuve numérique ?

Février 2023 — France. François Hollande, ancien Président de la République française, est piégé pendant une quinzaine de minutes lors d'une visioconférence. Deux humoristes russes — Vovan et Lexus — usurpent l'identité de l'ex-président ukrainien Porochenko grâce à un deepfake : visage et voix synthétisés en temps réel. Hollande croit discuter des accords de Minsk et de la guerre en Ukraine. Il ne réalisera le piège qu'après coup.

▶ Hollande piégé | Source : Euronews, avril 2023

Même une personnalité politique expérimentée n'a pas détecté le deepfake sur le moment.

Imaginez l'impact lorsqu'une vidéo ou un enregistrement arrive dans un dossier judiciaire.

QU'EST-CE QU'UN DEEPFAKE ?

Un **deepfake** est un contenu vidéo, audio ou photographique généré ou fortement modifié par intelligence artificielle (*deep learning*) afin de faire croire qu'une personne réelle a dit ou fait quelque chose qu'elle n'a jamais dit ou fait.

Étymologie : contraction de *deep learning* + *fake*

Aujourd'hui, ces technologies sont **accessibles à tous** et réalisables en quelques minutes avec un simple téléphone.

PROBLÉMATIQUE

« À l'ère de l'intelligence artificielle générative, à quelles conditions le juge peut-il encore se fier à ce qu'il voit, entend et lit ? »

PLAN DE L'INTERVENTION — 45 MINUTES

1

La preuve numérique est déjà là

Types de preuves, grille de lecture
pratique, cas WhatsApp

~8 min

2

Ce que l'IA change

Le faux crédible, le dividende du menteur, jurisprudence

~12 min

3

Comment raisonner et se protéger

Cadres juridiques, grille de prudence, expertise, limites

~12 min

4

Cas pratiques interactifs

3 cas — raisonnons ensemble

~8 min

✦ Conclusion et perspectives — ~5 min + Questions du public — ~15 min

1

La preuve numérique est déjà là

Ce que le juge reçoit chaque jour — et ce qu'il doit pouvoir apprécier

Deux grandes familles de preuves numériques

Distinction fondamentale : la preuve préexiste-t-elle, ou est-elle produite par un algorithme ?

PREUVES STOCKÉES

L'IA accède à un contenu préexistant et le restitue

E-mails
Contenu, en-têtes, métadonnées

Messages (WhatsApp, SMS)
Fils, horodatage, export

Documents électroniques
Contrats PDF, fichiers signés

Données techniques
Logs, IP, géolocalisation

Question clé : est-ce authentique et intègre ?

PREUVES GÉNÉRÉES

L'IA produit quelque chose de nouveau à partir de données

Images améliorées par IA
Résolution augmentée, netteté

Transcriptions automatiques
Audio → texte par algorithme

Analyses prédictives
Probabilités, corrélations

Reconstitutions visuelles
Scènes, visages, géolocalisation

Question clé : le processus est-il fiable ?

LOI 2008-08 — TRANSACTIONS ÉLECTRONIQUES

À l'instar de nombreux pays, le Sénégal s'appuie sur ses lois existantes — il n'existe pas de réglementation spécifique sur les deepfakes.

ART. 37 — Force probante de l'écrit électronique

L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier et a la même force probante, **sous réserve que puisse être dûment identifiée la personne dont il émane** et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

→ *Trois conditions :* identification de l'auteur, conservation pendant 10 ans, intégrité du contenu.

ART. 39 — Conflits de preuve

Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, **le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support.**

→ Le juge apprécie souverainement la fiabilité de la preuve numérique, quel que soit son support.

Grille de lecture : six critères d'appréciation

Grille inspirée du droit sénégalais de la preuve et des exigences procédurales — il ne s'agit pas d'un texte de loi

1 AUTHENTICITÉ

Qui est l'auteur réel ?

Identification de l'émetteur par éléments vérifiables (certificat, logs, recoupements)

2 INTÉGRITÉ

Le contenu a-t-il été altéré ?

Hash, empreinte numérique, horodatage, prestataire de confiance qualifié

3 TRAÇABILITÉ

Peut-on reconstituer le parcours ?

Chaîne de conservation documentée, de la création à la production en justice

4 LOYAUTÉ

Comment a-t-elle été obtenue ?

Absence de fraude, respect de la vie privée, proportionnalité des moyens employés

5 INTELLIGIBILITÉ

Peut-on comprendre comment elle a été produite ?

Le processus de génération est-il explicable ? Le juge peut-il exercer son contrôle ?

6 CONTRADICTOIRE

L'autre partie peut-elle la discuter ?

Accès effectif aux pièces, possibilité de contestation et de contre-expertise

Cas n° 1 — Messages WhatsApp et preuves de menaces

LES FAITS

Une victime de coups et blessures volontaires produit des captures d'écran de messages WhatsApp montrant des menaces proférées par le prévenu dans les jours précédant les faits. Le parquet les verse au dossier. La défense conteste l'authenticité.

LA DIFFICULTÉ JURIDIQUE

Une capture d'écran est une image. Elle ne contient ni métadonnées serveur, ni horodatage certifié, ni preuve d'intégrité du fil complet. Elle peut être recadrée ou modifiée.

CE QUE LE JUGE POURRAIT SE DEMANDER

— Qui a pris cette capture, et quand ?

— Le fil complet est-il accessible ?

— Peut-on obtenir un export technique ?

— Des éléments corroborants existent-ils ?

LA LEÇON — NUANCÉE

La capture d'écran n'est pas sans valeur probante. Elle peut constituer un commencement de preuve ou corroborer d'autres éléments du dossier. Mais en matière pénale, l'exigence est plus haute : la contestation d'authenticité impose au juge de rechercher des éléments de corroboration — export technique, relevé opérateur, témoignages concordants.

C'est une preuve stockée : la question est celle de l'authenticité et de l'intégrité, pas du processus de génération.

2

Ce que l'IA change

Un défi nouveau pour le raisonnement probatoire — mais pas une impasse

L'IA générative : des capacités de fabrication inédites

Ce que la technologie permet aujourd'hui — sans que cela signifie que toute preuve soit falsifiée

Images synthétiques

Personnes, documents, scènes photoréalistes n'ayant jamais existé

Clonage vocal

Reproduction fidèle d'une voix à partir de quelques secondes d'échantillon

Deepfakes vidéo

Substitution de visage, synchronisation labiale : la personne « dit » ce qu'elle n'a jamais dit

Documents générés

Contrats, correspondances d'apparence authentique, difficiles à distinguer

Faux échanges textuels

Conversations reconstituées, messages antidatés, fils modifiés

Métadonnées falsifiées

Géolocalisation, horodatage, identifiants : tous potentiellement manipulables

Le « dividende du menteur »

Chesney & Citron, 2019 — repris par le Laboratoire de cyberjustice de Montréal

L'existence même des technologies de falsification devient un argument de défense :
toute preuve numérique authentique peut désormais être contestée au motif qu'elle « pourrait » être un deepfake.

RISQUE 1 — Admettre un faux

Le juge accorde sa confiance à une preuve fabriquée. Conséquence : une décision fondée sur une base erronée, potentiellement irréversible.

RISQUE 2 — Rejeter un vrai

Le juge rejette une preuve authentique parce qu'elle est contestée comme deepfake. Conséquence : déni de justice, impunité de fait.

Le juge ne doit être ni naïf ni excessivement sceptique. Il doit calibrer sa vigilance.

CE QUE L'IA CHANGE — RÉPONSE RÉGLEMENTAIRE

La Commission de protection des données prend position

COLLECTE DE DONNÉES

L'exploitation massive de données personnelles à l'insu des personnes concernées, via les outils d'IA génératifs et les plateformes de deepfake.

ATTEINTES À LA PERSONNE

L'exposition des utilisateurs aux risques d'usurpation d'identité, de manipulation d'informations et d'atteintes irréversibles à leur réputation.

CONTENUS TROMPEURS

La création de contenus deepfake susceptibles de manipuler l'opinion, de nuire à la cohésion sociale et au vivre-ensemble.

La CDP appelle à une utilisation éthique de l'IA : vigilance des citoyens, responsabilité des créateurs de contenus, renforcement des mécanismes de détection par les plateformes numériques.

Source : Communiqué officiel CDP Sénégal — www.cdp.sn

Deux affaires fondatrices : quand l'IA entre dans le prétoire

Jurisprudence américaine — repères pour le débat international (Carbonell et al. 2026)

PREUVE IA ADMISE

US v. Lizarraga-Tirado

9th Circuit, 2015

Faits : Une épingle Google Earth placée automatiquement par l'algorithme est utilisée comme preuve de localisation géographique.

Question :
Cette épingle est un « témoignage machine » — produit sans intervention humaine. Est-ce recevable ?

Décision :
Admise. La fiabilité du logiciel Google Earth est considérée comme suffisamment établie.

→ Preuve générée par machine, admise sur la base de la fiabilité du processus

PREUVE IA EXCLUE

State of Washington v. Puloka

Washington, 2024

Faits : La police soumet une vidéo floue au logiciel Topaz Labs AI pour améliorer la résolution et identifier un suspect.

Question :
La vidéo « améliorée » par IA est-elle recevable comme preuve d'identification ?

Décision :
Exclue. Le processus d'amélioration n'est pas validé scientifiquement par les pairs.

→ Preuve générée par IA, exclue pour défaut de validation scientifique

Ce que l'IA change dans le raisonnement probatoire

AVANT L'IA GÉNÉRATIVE

- ✓ La source était déjà discutable, mais restait souvent un indice important.
- ✓ La cohérence interne pouvait suffire en l'absence de contestation sérieuse.
- ✓ L'apparence visuelle ou sonore avait une valeur indicative.
- ✓ Les contestations d'authenticité existaient, mais elles étaient moins fréquentes.

AVEC L'IA GÉNÉRATIVE

- → La source doit être davantage vérifiée.
- → La cohérence apparente peut être artificiellement produite.
- → L'apparence visuelle ou sonore ne suffit plus à elle seule.
- → Les contestations d'authenticité deviennent plus plausibles.
- → L'expertise technique doit être envisagée plus souvent lorsqu'un doute sérieux est soulevé.

L'IA ne supprime pas le raisonnement probatoire ; elle le rend plus exigeant.

3

Comment raisonner et se protéger

Cadres juridiques, grille de prudence et expertise technique

Cadres juridiques mobilisables

Hiérarchie des sources : du socle national à l'ouverture internationale

1

SOCLE NATIONAL SÉNÉGALAIS

Loi 2008-08 — Transactions électroniques (signature, preuve, écrit électronique) **Loi 2008-11** — Cybercriminalité (art. 431-7 à 431-67 CP : atteintes aux données, fraude, faux informatique) **Loi 2008-12** — Protection des données personnelles **Lois 2016-29/30** — Modifications du Code pénal et du Code de procédure pénale

2

CADRE AFRICAIN ET RÉGIONAL

Convention de Malabo (UA, 2014 — entrée en vigueur 2023) — cybersécurité et protection des données **Actes CEDEAO** — Directives sur la cybercriminalité et la protection des données

3

OUVERTURE INTERNATIONALE

Convention de Budapest (2001) + 2e Protocole additionnel (2022) — coopération transfrontalière **Recommandation UNESCO** sur l'éthique de l'IA (2021) — Lignes directrices sur l'IA dans les tribunaux (2025)

Grille de prudence judiciaire face à une preuve numérique

Repères méthodologiques pour structurer le raisonnement — non une checklist impérative

1

Qui est l'auteur présumé, et cette attribution est-elle vérifiable ?

Identification, certificat, recoupements

2

Le contenu est-il resté intègre depuis sa création ?

Hash, empreinte numérique, horodatage qualifié

3

Peut-on reconstituer le parcours de la pièce jusqu'au dossier ?

Chaîne de conservation, conditions de collecte et de transmission

4

L'obtention de la preuve est-elle loyale ?

Proportionnalité, respect de la vie privée, absence de fraude

5

Le processus de production est-il explicable et validé ?

Intelligibilité : le juge peut-il comprendre comment la preuve a été générée ? (cf. Puloka 2024)

6

Existe-t-il un risque crédible de fabrication ou d'altération par IA ?

Si oui → envisager une expertise.
Si incertitude → faisceau d'indices.

Lorsqu'un doute sérieux est soulevé, une vérification technique doit être sérieusement envisagée — dans la mesure du possible et du proportionné.

Expertise forensique et problème de la « boîte noire »

CE QUE L'EXPERTISE PEUT APPORTER

- ✓ Analyser les métadonnées et l'empreinte numérique d'un fichier
- ✓ Détecter certains artefacts de manipulation dans une image ou une vidéo
- ✓ Comparer une voix à un modèle de référence
- ✓ Vérifier la provenance et l'intégrité d'un document électronique

LES LIMITES À CONNAÎTRE

- — Aucun outil ne détecte les deepfakes avec 100 % de fiabilité
- — La course technologique avantage temporairement la fabrication
- — L'expertise a un coût et des délais parfois hors de portée
- — La détection dépend de la qualité initiale et de la compression du fichier

LE PROBLÈME DE LA « BOÎTE NOIRE » — Carbonell et al. 2026

Même si le résultat d'un algorithme est exact, l'impossibilité d'en expliquer le raisonnement crée un **déficit d'intelligibilité judiciaire**. Le juge ne peut pas exercer son contrôle si le processus est opaque. C'est précisément ce qui a conduit à l'exclusion de la preuve dans **Puloka (2024)** : la vidéo améliorée par IA était peut-être fidèle — mais personne ne pouvait l'expliquer.

Des outils pratiques pour les juges : les bench cards

AI Policy Consortium — National Center for State Courts (NCSC) & Thomson Reuters, 2025

PREUVE IA DÉCLARÉE

Présentée ouvertement comme créée ou modifiée par IA : vidéos de reconstitution d'accidents, outils d'analyse forensique, simulations.

La transparence sur les origines permet au juge de l'évaluer en connaissance de cause.

PREUVE IA NON DÉCLARÉE

Présentée comme authentique alors qu'elle est générée ou manipulée par IA : deepfakes vidéo, photos falsifiées, métadonnées altérées.

Le type le plus problématique : la détection et l'authentification sont particulièrement complexes en l'absence de déclaration.

Les bench cards fournissent aux juges des questions structurées sur la source, la chaîne de conservation et les altérations possibles — pour une décision éclairée face à une preuve potentiellement générée par IA.

Source : AI Policy Consortium — NCSC & Thomson Reuters (2025) — ncsc.org

Cas concret — L'enregistrement audio “amélioré” par IA

LES FAITS

Dans une affaire de corruption, la partie civile produit un enregistrement audio censé prouver un pacte de corruption. L'enregistrement original était de mauvaise qualité. La partie l'a “amélioré” via un outil IA (réduction de bruit, amplification vocale) avant de le produire. La défense conteste la fiabilité du procédé.

LA DIFFICULTÉ JURIDIQUE

C'est une PREUVE GÉNÉRÉE. L'IA a transformé le signal audio original — elle ne l'a pas seulement restitué. Le résultat peut être plus audible, mais est-il toujours fidèle ? Le processus de traitement algorithmique a-t-il altéré, amplifié ou supprimé certains éléments sonores ?

CE QUE LE JUGE POURRAIT SE DEMANDER

— Quel outil a été utilisé pour le traitement ?
— L'enregistrement original a-t-il été conservé ?
— Le processus de traitement est-il documenté et reproductible?
— Un expert peut-il analyser l'original et le traité côte à côte ?

LA LEÇON — NUANCÉE

L'enregistrement “amélioré” est une preuve générée : c'est le critère d'intelligibilité qui s'applique en premier. Si le prestataire ne peut documenter son algorithme, si l'original n'est plus accessible, si aucun expert ne peut reproduire le traitement — la valeur probante est sérieusement compromise, quelle que soit la qualité sonore obtenue.

C'est une preuve générée : le critère déterminant n'est pas l'authenticité de l'original, mais l'intelligibilité du processus de transformation algorithmique. Cf. State of Washington v. Puloka (2024).

Cas concret n° 2 — L'enregistrement audio litigieux

LES FAITS

Dans un litige civil, une partie produit un enregistrement audio d'une conversation où l'adversaire reconnaît une dette. L'enregistrement a été réalisé à l'insu de l'interlocuteur.

LA DOUBLE DIFFICULTÉ

Deux questions se posent simultanément : la loyauté de l'obtention (enregistrement clandestin — art. 363 bis CP) et l'authenticité de la voix (risque de clonage vocal par IA).

CE QUE LE JUGE POURRAIT SE DEMANDER

— L'enregistrement a-t-il été obtenu loyalement ?

— La voix est-elle authentique ou clonée ?

— Un expert peut-il analyser le fichier source ?

— D'autres éléments corroborent-ils le contenu ?

LA LEÇON — NUANCÉE

L'enregistrement clandestin n'est pas nécessairement irrecevable en droit sénégalais — le juge apprécie la proportionnalité. Quant à l'authenticité vocale, si un doute sérieux est soulevé, une expertise doit être envisagée.

L'IA ajoute une couche de complexité à un problème probatoire qui existait déjà — elle ne le crée pas.

Cas concret n° 3 — La signature électronique contestée

LES FAITS

Une entreprise produit un contrat signé électroniquement via une plateforme en ligne. L'adversaire conteste : selon lui, le contrat a été signé à son insu ou modifié après signature.

LA DIFFICULTÉ JURIDIQUE

Toutes les signatures électroniques n'offrent pas les mêmes garanties. Une signature simple (case à cocher) diffère fondamentalement d'une signature qualifiée avec certificat cryptographique (Loi 2008-08).

CE QUE LE JUGE POURRAIT SE DEMANDER

— Le prestataire est-il certifié ?

— L'horodatage est-il qualifié ?

— Le certificat de signature est-il traçable ?

— Les logs du prestataire sont-ils disponibles ?

LA LEÇON — NUANCÉE

La signature électronique doit être appréciée à partir des garanties techniques et organisationnelles qui entourent son attribution et son intégrité. La qualité de la chaîne technique détermine la force probante.

La présomption d'intégrité dépend du niveau de garantie. Si le prestataire n'est pas certifié, la charge de la preuve revient au producteur.

4

Cas pratiques interactifs

Raisonnons ensemble — le juge face à la preuve numérique

CAS PRATIQUE N° 1

Affaire de harcèlement — Conversation WhatsApp versée aux débats

FAITS

Une plaignante produit des captures d'écran WhatsApp avec son supérieur hiérarchique. Les messages contiennent des propos à caractère sexuel. Le défendeur nie et allègue un montage. Aucune des parties n'a conservé l'export officiel.

Q1 **La capture d'écran seule peut-elle fonder une conviction ?**

→ Pas à elle seule — absence de métadonnées serveur. Mais elle n'est pas sans valeur : elle peut constituer un commencement de preuve.

Q2 **Quels éléments complémentaires le juge pourrait-il demander ?**

→ Export officiel WhatsApp, relevé opérateur, données de connexion, témoignages concordants.

Q3 **La contestation du défendeur suffit-elle à écarter la preuve ?**

→ Non automatiquement. Le juge évalue la crédibilité globale et le faisceau d'indices.

Q4 **Une expertise est-elle possible sur une simple capture ?**

→ Très limitée sur la capture. L'expertise sur l'appareil original serait plus pertinente, si disponible.

CAS PRATIQUE N° 2

Affaire pénale — Vidéo de surveillance et allégation de deepfake

FAITS

Affaire de trafic de drogue : le parquet produit une vidéo de surveillance montrant le prévenu. La défense allègue un deepfake. L'expertise conclut à une « probabilité élevée d'authenticité » — sans certitude absolue.

Q1

Une « probabilité élevée d'authenticité » suffit-elle en matière pénale ?

→ Le juge forme son intime conviction. L'expertise éclaire mais ne remplace pas l'appréciation souveraine.

Q2

Quel poids accorder à une contestation non étayée techniquement ?

→ La simple allégation de deepfake ne suffit pas. La contestation doit être crédible et, si possible, appuyée par des éléments.

Q3

Comment consolider la preuve vidéo dans le dossier ?

→ Recouper : témoignages, données de connexion, preuves financières, géolocalisation.

Q4

La vidéo doit-elle être écartée si le doute subsiste ?

→ Pas nécessairement. Appréciation souveraine + faisceau d'indices. Le doute raisonnable reste le standard.

CAS PRATIQUE N° 3

Affaire pénale — Vidéo floue « améliorée » par intelligence artificielle

FAITS

Agression nocturne filmée par une caméra de mauvaise qualité. L'enquêteur utilise un logiciel d'amélioration vidéo par IA pour clarifier l'image et identifier un suspect. La défense conteste : l'image « améliorée » n'est pas l'image originale.

Q1

La vidéo améliorée par IA est-elle une preuve stockée ou générée ?

→ C'est une preuve GÉNÉRÉE : l'IA a produit une nouvelle image à partir de données. Ce n'est plus l'enregistrement original.

Q2

Le processus d'amélioration doit-il être validé scientifiquement ?

→ Oui — cf. Puloka 2024 (Washington) : preuve exclue pour absence de validation scientifique par les pairs du logiciel IA.

Q3

Le juge peut-il quand même utiliser la vidéo originale ?

→ Oui. La vidéo originale reste une preuve stockée, évaluable selon les critères classiques, même si floue.

Q4

Comment le juge doit-il raisonner face à ce type de preuve ?

→ Appliquer le critère d'intelligibilité : le processus est-il explicable ? Sinon, la preuve générée ne peut fonder une conviction à elle seule.

Conclusion et perspectives

Ce que le praticien du droit doit retenir

Trois messages essentiels

1

La preuve numérique est un enjeu qui exige une méthode

Elle est déjà partout dans le contentieux. L'IA en fait un enjeu plus complexe. Ce n'est pas une raison de s'en méfier par principe — c'est une raison de structurer son raisonnement.

2

Le juge dispose de cadres, d'outils et de critères

Cadres juridiques sénégalais et régionaux, grille de six critères, expertise forensique, faisceau d'indices — et désormais le critère d'intelligibilité pour les preuves générées par IA.

3

L'enjeu est aussi institutionnel

Former les magistrats, doter les juridictions d'accès à l'expertise, développer la coopération régionale : c'est un investissement dans la crédibilité de la justice à l'ère numérique.

« Le juge a toujours été le gardien de la vérité judiciaire.

À l'ère de l'intelligence artificielle, cette mission n'a pas changé.

Elle exige simplement de lui une vigilance nouvelle,
des outils nouveaux, et surtout —
une méthode plus rigoureuse. »

Merci de votre attention.
Place aux questions.

Gora Ngom | gora.ngom@brio-academy.com | CFJ Sénégal — 14 avril 2026