GROUPE DE RECHERCHE
ET D'INFORMATION
SUR LA PAIX ET LA SÉCURITÉ

•

Bâtiment Mundo-Madou
Avenue des Arts 7-8,
1210 Bruxelles, Belgique.
Tél. : +32 (0) 0484 942 792
Courriel : admi@grip.org
Internet : www.grip.org
Twitter : @grip_org
Facebook : GRIP.1979

Éclairage

Enquêter en ligne : la justice internationale face aux défis des preuves numériques en sources ouvertes

Philippine Sottas

8 septembre 2022

Le 28 février 2022, Karim A. Khan, procureur de la Cour pénale internationale (CPI), a annoncé l'ouverture d'une enquête sur la situation en Ukraine[1]. Les investigations, qui ont officiellement débuté le 2 mars 2022, intègrent des vidéos, des photos et autres types de publications diffusées sur des réseaux sociaux et des plateformes numériques (*Facebook*, *YouTube*, *Twitter* ou encore *TikTok*). Si certains États sont habitués à l'exercice (la Finlande, la Suède, l'Allemagne et les Pays-Bas, par exemple), la CPI est peu familière avec la démarche de récolte de documents « *open source* » (ou OSINT, pour *Open Source INTelligence*) dans le cadre de ses enquêtes portant sur des crimes contre l'humanité, des crimes de guerre, ou des crimes de génocide[2]. Pourtant, l'utilisation de vidéos, photos et autres documents numériques publiés sur les réseaux sociaux comme éléments de preuve est amenée à se répandre. Dans son « Plan stratégique 2016-2018 », le Bureau du procureur de la CPI note ainsi que « *l'accès à Internet par les victimes, les témoins et les auteurs des crimes crée un environnement dynamique pour surveiller et confirmer la commission de crimes relevant de la compétence de la Cour* »[3].

La mobilisation des sources ouvertes présente de nombreux avantages. Elle permet, d'une part, de réduire les coûts des enquêtes, mais aussi (et surtout) de contourner les problèmes d'accès au terrain. Les observations sur site sont, en effet, souvent compromises tant parce que des hostilités sont encore en cours que parce que l'État sur le territoire duquel les crimes ont été commis refuse de coopérer avec la CPI[4]. Malgré ces avantages, le recours à des preuves numériques identifiées à distance dans le cadre de procès pénaux internationaux n'est pas sans poser de sérieux défis.

ÉCLAIRAGE – 8 septembre 2022

SOTTAS Philippine. « *Enquêter en ligne : la justice internationale face aux défis des preuves numériques en sources ouvertes* », Éclairage du GRIP, 8 septembre 2022, Bruxelles.

http://www.grip.org/enqueter-en-ligne-la-justice-internationale-face-aux-defis-des-preuves-numeriques-en-source-ouverte

Cet *Éclairage* passe en revue les difficultés rencontrées par les enquêteurs et autres acteurs de la justice internationale dans l'identification et l'utilisation des preuves numériques collectées en sources ouvertes. Il retient, pour fin de classification, quatre principaux types de défis, qui tiennent 1) à la collecte de l'information, 2) à l'archivage des données, 3) à l'authentification des documents et 4) aux risques que soulève l'utilisation de ces informations en matière d'impartialité de la justice pénale internationale et du droit à un procès équitable. L'analyse successive des éléments propres à ces quatre catégories permet en conclusion de questionner la pertinence de cadrer davantage ou non, par des normes juridiques dédiées, l'usage des preuves OSINT par les acteurs de la justice pénale internationale.

La collecte : censure privée et étatique des contenus

La collecte de l'information désigne la phase de recherche visant à rassembler le plus grand nombre possible d'éléments susceptibles de constituer des preuves. Elle peut être menée par différents acteurs. Il s'agit le plus souvent, d'une part, des agences étatiques et, d'autre part, d'organismes issus de la société civile. À titre d'illustration, en 2014, l'ONG *Mnemonic* s'est trouvée à l'initiative du projet « Syrian Archive », une plateforme créée dans le but de récolter, rassembler et conserver divers types de documents digitaux renseignant des violations des droits de la personne commis durant le conflit[5]. Depuis, cette ONG a mis en place des plateformes similaires en lien avec la guerre au Yémen et la situation au Soudan[6]. Certains États européens (l'Allemagne et la Suède, notamment) ont également procédé à des collectes similaires lorsque leurs juridictions ont été amenées à juger de crimes internationaux sur la base de la compétence universelle[7].

Concrètement, la collecte de l'information peut prendre deux formes principales : soit les informations sont directement envoyées aux organisations se chargeant de les récolter, soit elles font l'objet d'un processus de recherche systématique sur les réseaux sociaux. Dans un cas comme dans l'autre, des problèmes surgissent.

Le premier tient aux politiques de contrôle des contenus des réseaux sociaux et autres plateformes de partage en ligne. La phase de collecte peut être interrompue par les compagnies privées. Selon les règles et les algorithmes propres à chaque réseau, les images et/ou propos « *violents ou graphiques* » sont souvent rapidement supprimés[8]. On pense ici aux processus de modération des contenus en vigueur sur *YouTube*, *Facebook*, ou encore *Twitter*, par exemple. Les algorithmes signalant la présence de contenus problématiques sont susceptibles d'entraîner la disparition de preuves avant qu'elles n'aient pu être recueillies et archivées sur d'autres plateformes accessibles aux enquêteurs. Conscient de ce problème, le Bureau du procureur de la CPI a d'ailleurs déclaré qu'il « *poursuivra ses échanges avec les fournisseurs d'accès à Internet pour*

identifier les moyens de préserver des informations en ligne accessibles au public »[9]. On note au passage que parfois les législations nationales (en France, notamment) exigent des fournisseurs qu'ils conservent les données de leurs utilisateurs, afin d'être en mesure de les transmettre à des services de police si besoin[10].

Dans certaines situations, la suppression de contenu n'est pas le fait des compagnies privées, mais des États eux-mêmes. Il est déjà arrivé que des États suspendent leurs services numériques afin de limiter la prolifération d'images qui pourraient porter atteinte à leur réputation sur la scène internationale. En septembre 2019, le gouvernement du Bangladesh a ainsi coupé l'accès à Internet au sein des camps de réfugiés rohingyas. Le service ne fut rétabli que près d'un an plus tard, le 29 août 2020, à la suite d'appels répétés des Nations unies et des groupes de défense des droits humains[11]. Justifiant cette interruption par des mesures de sécurité nationale[12], les autorités ont empêché le Mécanisme indépendant des Nations unies pour le Myanmar de récolter des informations qui auraient permis de documenter les allégations de génocide à l'encontre du pouvoir birman et/ou de mauvais traitements au sein des camps de réfugiés.

L'archivage : quand la masse force à la sélection

Dans le cadre de ses projets de collecte et de conservation, *Mnemonic* décrit sa méthode comme étant basée sur *l'Electronic Discovery Reference Model* développé par la faculté de droit de l'université Duke, aux États-Unis[13]. Dans ce modèle, l'information est collectée avant d'être archivée, c'est-à-dire conservée dans un fond dont elle pourra éventuellement être re-extraite afin de servir de preuve dans le cadre d'un procès. L'archivage s'effectue généralement en transférant les documents récoltés sur des plateformes dédiées ou, à tout le moins, préservées des mécanismes de modération et de censure. Le procédé limite les risques de destruction et d'éventuelles manipulations ou altérations des données. Dans la pratique, les ONG cherchant à documenter la commission de crimes internationaux préfèrent accumuler autant d'informations que possible afin de ne pas préjuger de leur authenticité ou de leur valeur probante avant qu'elles n'aient fait l'objet d'un examen approfondi. Il s'en suit qu'une quantité impressionnante de documents se retrouve stockée sur des plateformes de conservation. Les projets « *Syrian Archive* » et « *Yemeni Archive* » indiquent ainsi respectivement détenir 3 578 591 et 637 197 vidéos[14]. Le nombre de documents conservés présente le risque que les vidéos, photos et autres publications réellement intéressantes se noient dans une masse d'information. Dit autrement, certaines preuves pourraient ne pas être identifiées et donc ne jamais être exploitées.

Cet élément lié à la conservation conditionne indirectement les phases de collecte et d'authentification. Anticipant sur les problèmes liés à la masse des données, les acteurs qui documentent les crimes opèrent une sélection *a priori* dès la phase de collecte. En d'autres termes, ils établissent en amont du processus de stockage une hiérarchie des sources en identifiant et priorisant celles qu'ils considèrent comme étant « *fiables* ». Il s'agit le plus souvent de journalistes, de groupes médiatiques locaux et étrangers, d'organisations de défense des droits de la personne présentes sur le terrain et de « *citoyens reporters* »[15]. Ils n'indiquent néanmoins pas selon quels critères ils établissent qu'une source est plus crédible qu'une autre ; la notion de « *citoyen reporter* » étant d'ailleurs éminemment floue.

Ainsi, tant la phase de collecte que celle de l'archivage comportent dans la pratique des biais susceptibles, d'une part, de ne permettre par la suite qu'une représentation partielle des faits, mais aussi, d'autre part, de refléter une tendance à documenter en priorité et majoritairement les exactions de certaines parties au conflit plutôt que celles des autres. Ce double biais a notamment poussé certains à questionner la légitimité de la Commission pour la justice internationale et la responsabilité (CIJA), organisation non gouvernementale créée en 2011 pour collecter des preuves de violations en Syrie. Par exemple, l'universitaire Melinda Rankin, dénonce le fait que la Commission n'enquête que sur deux groupes, l'État islamique et le gouvernement syrien[16], alors que son mandat devrait s'étendre à l'intégralité des acteurs étatiques et non étatiques impliqués dans le conflit. L'archivage d'informations issues de sources ouvertes reposant majoritairement sur le travail des ONG, le risque d'une approche partiale et ciblée sur certaines parties au conflit est réel.

L'authentification : manipulations, *deepfake* et anonymat

L'authentification a pour objectif d'évaluer et de garantir l'intégrité des documents recueillis, ainsi que la fiabilité et la véracité des faits qui y sont relatés. Le processus présente des difficultés qui, tout en n'étant pas spécifiques à la nature numérique des informations, sont augmentées lorsque les enquêteurs sont confrontés à ce type de documents.

Une première difficulté est liée à l'identification de la source et du contenu original. Dans la majorité des cas, les vidéos, photos ou enregistrements postés sur Internet ne le sont pas dans leur forme authentique. Pour que l'information soit identifiée comme authentique, celle-ci doit contenir le lien, la date, l'heure et l'identité de l'auteur du document[17]. Seulement, les contenus sont rarement relayés avec l'intégralité de ces métadonnées qui permettent aux enquêteurs de retracer l'origine d'une pièce d'intérêt[18]. À titre d'exemple, lorsqu'on importe une photo sur Facebook, certaines métadonnées de celle-ci sont supprimées et remplacées par les codes du réseau social. C'est le cas, par exemple, des données de localisation[19].

Encadré 1. L'ombre de la désinformation

Les conflits vont souvent de pair avec des campagnes de désinformation. Avant vérification et authentification, les informations relayées sur les réseaux sont susceptibles d'avoir été modifiées voir fabriquées par des internautes, mais aussi par des États tentant d'imposer un narratif favorable à leurs intérêts. Il n'existe pas de conflit qui ne soit soumis à des campagnes de propagande de la part d'acteurs étatiques ou non étatiques. Ces pratiques renvoient notamment à une guerre des images et du numérique. Elles fragilisent le travail de la justice et compliquent l'authentification des données.

En avril 2022, dans le nord du Mali, récits et contre-récits ont été utilisés pour justifier la présence de corps enterrés près de la base de Gosse. Des images du charnier ont tout d'abord été relayées par un compte Twitter créé en janvier 2022 appartenant à un certain Dia Diarra. Sur son compte, celui-ci se présente comme un « *ancien militaire* » et « *patriote malien* ». L'utilisateur accuse les soldats français d'être à l'origine de ces exactions. Répondant à ces accusations, l'armée française a indiqué avoir filmé à l'aide d'un drone ce qu'elle affirme être des mercenaires russes du Groupe Wagner couvrant les corps de sable, preuve selon elle d'une « *opération de manipulation destinée à incriminer Barkhane*[20] ». Sans le contrôle du drone français, les images initialement diffusées auraient pu faire l'objet d'une enquête préliminaire pour crimes de guerre.

Ce cas illustre un des pièges que doivent contourner les enquêteurs agissant dans la perspective d'ouvrir des poursuites internationales. Il en existe d'autres en matière de propagande. Par exemple, ces activités font aussi parfois intervenir des « bots », ces comptes automatisés qui partagent du contenu orienté tentant d'attirer l'attention en essayant de provoquer des réactions en chaîne dans la diffusion toujours plus large et plus rapide de contenus manipulés.

Il est pourtant primordial de retrouver le contenu original afin de s'assurer que les informations n'aient pas été mal contextualisées ou modifiées a posteriori. Les avancées technologiques facilitent en effet grandement la falsification des contenus. Les *deepfakes* — images et vidéos ultra réalistes créées grâce à des algorithmes d'apprentissage automatique —, en particulier, préoccupent de plus en plus la justice. À terme, l'accroissement du nombre de contenus basés sur l'intelligence artificielle pourrait éroder la confiance dans les preuves numériques issues de sources ouvertes. Cela est d'autant plus plausible que les outils véritablement performants permettant de détecter les contrefaçons numériques pourraient, du fait de leur coût, ne pas être accessibles aux ONG qui récoltent et archivent les éventuelles preuves. Une autre limitation risque aussi de résulter de la volonté de certains États d'encadrer ou prohiber l'accès aux technologies de décryptage et cryptage en raison des applications militaires dont celles-ci sont susceptibles de faire l'objet. Même lorsqu'il est possible de retrouver le document original, le problème de l'anonymat de la source d'information peut faire son apparition. Il n'est pas rare que les auteurs des contenus postés sur les plateformes en ligne soient anonymes. Or, la CPI est plutôt réticente à admettre

des preuves dont l'auteur ne peut être identifié. Ainsi, dans l'affaire contre l'ancien président ivoirien Laurent Gbagbo[21], la Cour a estimé que, « *en de pareils cas, la Chambre n'est pas en mesure d'apprécier la fiabilité de la source, ce qui la met dans l'impossibilité de déterminer la valeur probante à accorder aux informations*[22] ». Les juridictions pourraient donc être confrontées à un dilemme : celui de protéger l'anonymat d'une source ou de rendre, malgré les risques pour sa sécurité, son identité publique afin de pouvoir utiliser l'information lors d'un procès. De cette décision pourraient naître des risques concernant la protection du témoin et de sa vie privée.

La société civile a soumis des recommandations spécifiques sur ces questions d'authentification. Collaborant avec le Haut-Commissariat des Nations unies aux droits humains, le Centre des droits humains de l'université de Californie à Berkeley a produit un protocole décrit comme « *les premières lignes directrices mondiales pour l'utilisation d'informations en ligne publiquement disponibles* »[23]. Celui-ci propose des normes d'identification, de collecte, de préservation et d'analyse concernant les preuves numériques issues de sources ouvertes. Plus spécifiquement, concernant les preuves vidéographiques, photographiques ou audiographiques le protocole recommande de « *prouver leur origine et leur intégrité* »[24], les informations ne devant pas être modifiées numériquement. Ce protocole n'introduit aucune norme contraignante, mais il s'accompagne d'une première étape de formation des organismes d'enquête, qu'il s'agisse de la CPI, des commissions d'enquête des Nations unies ou des groupes de défense des droits de la personne.

Tout au long de la procédure judiciaire, la quantité de données brutes archivées représente un défi de taille au niveau du traitement, de l'analyse et de l'authentification. Le processus d'authentification est chronophage et demande des moyens humains, techniques et financiers non négligeables ; moyens dont les ONG, les juridictions et autorités nationales aussi bien qu'internationales ne disposent pas nécessairement. Ici se pose aussi la question des compétences requises pour traiter des développements numériques, tant du côté de la Cour que de la Défense.

Le poids des images, obstacle à l'impartialité de la justice internationale

L'utilisation de sources ouvertes pose la question de l'impact des images sur le choix des juridictions internationales de se saisir de telles situations plutôt que de telles autres. La justice internationale, malgré son objectif initial d'impartialité, est le lieu d'influences politico-médiatiques. Nul conflit armé n'est à l'abri de campagnes visant à imposer des narratifs spécifiques (voir l'encadré ci-dessus). Les parties au conflit tentent, par le biais médiatique, de légitimer leurs actions ou de se dédouaner d'éventuelles accusations. Le cas du conflit en Ukraine est

particulièrement révélateur de ces entreprises gouvernementales. On observe que dans l'objectif de documenter les exactions russes, les autorités nationales ukrainiennes ont créé un site web permettant aux témoins d'envoyer de potentielles preuves numériques. Hormis le travail des enquêteurs nationaux et internationaux, la collecte de preuves repose donc sur des utilisateurs d'Internet. L'application *eyeWitness to Atrocities* a ainsi récolté plus de 10 000 vidéos, photographies et fichiers audio[25].

Parmi les nombreuses images retraçant le conflit en cours en Ukraine, certaines ont particulièrement marqué l'opinion publique, comme celles documentant le massacre de Butcha[26]. Parallèlement, les autorités russes se sont appuyées sur ces mêmes images pour critiquer l'utilisation de l'OSINT dans le cadre du conflit. Le narratif russe s'est évertué à contrer les allégations de crimes de guerre, affirmant que l'imagerie satellite était faussée et les preuves falsifiées[27]. La démarche russe consiste à remettre en cause la crédibilité des informations issues de sources ouvertes afin de discréditer les images et réfuter les allégations. Cette propagande russe est soutenue par divers relais médiatiques, dont un site particulièrement actif nommé *War on Fakes*[28]. Le public de ce site nationaliste, que l'on pourrait penser à première vue destiné à la communauté russophone, est en réalité international puisque la page se décline en plusieurs langues : anglais, français, allemand, espagnol, chinois et arabe.

Si les médias occidentaux ont relayé une masse importante d'informations documentant de potentiels crimes de guerre commis par des soldats russes, la publication d'informations mettant en cause des soldats ukrainiens s'est faite plus discrète. Les réactions internationales et ukrainiennes lorsque sont abordées les exactions de soldats ukrainiens révèlent l'influence émotionnelle des images et des narratifs en temps de conflit. Un rapport d'Amnesty International[29], publié le 4 août 2022, et accusant les forces armées ukrainiennes de mettre en danger des vies civiles a ainsi provoqué des vives réactions. L'ONG, dont la démarche vise à documenter les exactions de l'ensemble des acteurs gouvernementaux dans le conflit ukrainien, a d'ailleurs dû s'excuser pour la « colère » provoquée par sa publication[30]. Les critiques en provenance du pouvoir ukrainien ont été particulièrement acerbes, Kiev affirmant qu'on ne peut décemment pas comparer un pays agressé et un pays agresseur et que la démarche d'Amnesty International fait *in fine* le jeu de la propagande russe. Il est apparemment nécessaire de rappeler ici que le droit international humanitaire s'applique à toutes les parties au conflit armé, tant au pays en position de légitime défense, l'Ukraine, qu'à l'envahisseur, la Russie.

D'une manière finalement assez prévisible, tant le rapport d'Amnesty International en lui-même que les réactions qu'il a suscitées soulignent le rôle que l'OSINT peut jouer dans la lutte contre l'impunité et la poursuite de responsables de crimes internationaux. Il convient de faire la part des choses entre, d'un côté, les observations factuelles rigoureusement documentées et, de l'autre, les

stratégies de communication déployées par les parties au conflit pour imposer leur narratif sur la guerre et influencer les perceptions de ce qui est légitime ou non. Il importe également de rappeler qu'il n'appartient à aucune des parties en conflit de déterminer quelles sont les procédures de collecte de preuves potentielles qui sont légitimes et quelles sont celles qui ne le sont pas.

Par ailleurs, le fait que des informations soient plus relayées que d'autres sur les plateformes numériques ou dans les médias, qu'un conflit retient une attention médiatique plus grande qu'un autre, ou qu'une des forces armées suscite davantage la sympathie, sont des éléments susceptibles de participer à une pression politique et sociétale visant à engager des procédures judiciaires dans certains cas et moins, voire pas, dans d'autres. Ces biais contribuent malheureusement à renforcer l'idée que la justice pénale internationale est à deux vitesses, subjective, sélective et partiale — en bref, une « justice du vainqueur ».

La problématique de l'impartialité dans le choix des poursuites amène aussi celle des droits de la défense et du droit au procès équitable[31]. Afin d'assurer l'impartialité du processus judiciaire, l'enquête doit être faite à charge et à décharge. Le Code de conduite du Bureau du procureur de la CPI précise en effet que : « *[c]onformément à son obligation d'établir la vérité […], le Bureau enquête tant à charge qu'à décharge*[32] ». Toutefois, les organisations de la société civile — acteurs incontournables dans l'identification de potentielles preuves et animés par la volonté de lutter contre l'impunité — ont souvent un parti pris pour les victimes présumées. Nonobstant son caractère louable, cette ambition induit une orientation susceptible de compromette la défense des prévenus[33]. Les ONG peuvent avoir une propension à enquêter et récolter des preuves davantage à charge qu'à décharge. La justice pénale internationale doit donc aborder ces éléments avec une certaine distance et en veillant à combler les lacunes affectant le processus de collecte. À cet égard il faut d'ailleurs souligner que, si elle a déjà admis des rapports émanant d'ONG comme éléments de preuve, la CPI estime généralement que ceux-ci ne sont admissibles que lorsqu'ils corroborent des documents en provenance de sources plus officielles (notamment onusiennes) et/ou les observations des enquêteurs sur place[34]. Reste à voir si cette posture sera maintenue face à l'essor de l'OSINT et des possibilités qu'il offre à la justice pénale internationale dans l'accomplissement de ses missions.

Conclusion : de la nécessité d'un cadre juridique plus strict ?

La situation en Ukraine interroge sur le poids de la guerre des images et autres jeux d'influences sur la justice pénale internationale. Elle met plus que jamais en lumière la place grandissante qu'ont les documents numériques postés sur les réseaux sociaux dans les processus judiciaires. Ce phénomène est aussi voué à accroître la quantité d'acteurs impliqués, directement ou indirectement, dans les investigations pour génocide, crimes contre l'humanité ou crimes de guerre. Dit autrement, il amplifie ce que certains ont décrit comme une « externalisation »

du travail d'enquête de la CPI[35]. Il pose aussi des défis particuliers à la justice internationale, en particulier en ce qui concerne la collecte, l'archivage et l'authentification des potentielles preuves ; défis qui, à leur tour, questionne le poids des émotions dans les pratiques judiciaires.

Chacun à leur manière, ces défis mettent en exergue le risque que le traitement des informations numériques soit biaisé et le « régime » d'improvisation qui entoure leur utilisation lors d'éventuelles poursuites. S'il existe bien des règles relatives à l'admissibilité des preuves devant les juridictions pénales internationales[36], celles-ci ne prennent pas en compte les spécificités liées à l'OSINT. Bien que la société civile ait commencé à se saisir de la question, ces recommandations n'ont pas de force de loi. En somme, aucun principe contraignant clairement dédié aux preuves numériques collectées en sources ouvertes n'existe.

La montée en puissance de ce type de document dans l'administration de la justice pénale internationale pose néanmoins la question de savoir si la formulation et l'adoption de tels principes ne seraient pas souhaitables. Le but serait d'éviter ou de limiter certains des écueils mis en exergue précédemment. Il convient, toutefois, de se montrer prudent avec cette approche.

Il faut, en particulier, distinguer la situation des juges amenés à décider si une preuve est ou non admissible de celle des acteurs (étatiques, internationaux et non gouvernementaux) impliqués dans la collecte, l'archivage et l'authentification des documents mis en ligne. Alors qu'un meilleur cadrage de l'action des seconds permettrait de légitimer l'utilisation de sources numériques en les rendant plus fiables, la plus-value est moins claire pour les premiers. De fait, il faut tout d'abord souligner que les règles relatives à l'admissibilité des preuves et la jurisprudence permettent déjà de poser certains garde-fous. Comme mentionné précédemment, c'est le cas en ce qui concerne l'anonymat et le poids à donner aux informations en provenance des ONG. Établir des règles supplémentaires pourrait substantiellement réduire la marge de manœuvre des juges. Loin de compromettre l'action des tribunaux pénaux internationaux, cette flexibilité est peut-être ce qui leur permet d'opérer dans un contexte où leur budget et accès au terrain est limité.

Il n'en demeure pas moins que les institutions pénales internationales doivent avoir pleinement conscience des biais et jeux d'influence qui teintent la mobilisation des preuves numériques dans les affaires de droit international au risque de manquer à une obligation fondamentale : le traitement équitable des justiciables.

***

Auteure

Philippine Sottas est assistante de recherche au GRIP. Elle est doctorante contractuelle au Laboratoire de Droit International et Européen (LADIE) de l'Université Côte d'Azur et diplômée d'un master en Sécurité internationale, Défense et Intelligence économique

---

1. CPI, *Déclaration du Procureur de la CPI, Karim A.A. Khan QC, sur la situation en Ukraine* , 28 février 2022.
2. AKSAMITOWKA Karolina, « Digital evidence in domestic core international crimes prosecutions: lessons learned from Germany, Sweden, Finland and the Netherlands », *Journal of International Criminal Justice*, vol. 19, n° 1, 2021, p. 189-211.
3. CPI, Bureau du procureur, *Plan Stratégique 2016-2018 du Bureau du Procureur*, Document officiel, 8 juillet 2015, § 23, p. 12.
4. Le gouvernement du Myanmar a ainsi refusé à plusieurs reprises l'accès au terrain à des observateurs extérieurs indépendants. Nations unies, « UN rights expert "disappointed" by Myanmar's decision to refuse visit », *UN News*, 20 décembre 2017.
5. DEUTCH Jeff et HABAL Hadi, « The Syrian archive: a methodological case study of open-source investigation of state crime using evidence from social media platforms », *State Crime Journal*, vol. 7, n° 1, 2018, p. 46-76.
6. Pour avoir accès à ces plateformes : Yemeni Archive et Sudanese Archive.
7. HEIKKILÄ Mikaela, « The criminalisation and prosecution of international core crimes in Finland », *Scandinavian Studies in Law*, vol. 66, 2020, p. 14.
8. ASHER-SCHAPIRO Avi, « YouTube and Facebook are removing evidence of atrocities, jeopardizing cases against war criminals », *The Intercept*, 2 novembre 2017.
9. CPI, Bureau du Procureur, *Plan stratégique 2019-2021*, 17 juillet 2019, § 55, p. 35.
10. France, Loi n° 2004-575 pour la confiance dans l'économie numérique, 21 juin 2004, art. 6.
11. SAKIB Najmus, «Internet, mobile network for Rohingya refugees », *Anadolu Agency*, 29 août 2020.
12. *Ibid*.
13. Syrian Archive, *Open source tools and methods for open source investigation*, consulté le 2 juillet 2022.
14. Ces chiffres sont ceux communiqués par les plateformes Yemeni Archive et Sudanese Archive.
15. Haut-Commissariat des Nations unies aux Droits de l'Homme, *Berkeley Protocol on digital open source investigations: a practical guide on the effective use of digital open source and information in investigating violations of international criminal human rights and humanitarian law*, 3 janvier 2022.
16. RANKIN Melinda, « The future of international criminal evidence in new wars? The evolution of the Commission for international justice and accountability (CIJA) », *Journal of Genocide Research*, vol. 20, n° 3, 2018, p. 392-411.
17. Trial International, « La preuve audiovisuelle devant les instances internationales : techniques et admissibilité », *Manuel à l'usage des praticiens*, 2019.
18. International Press Telecomunications Council, « Many social media sites still remove image rights information from photos », *Report*, 19 janvier 2016.
19. « Facebook épinglé par Apple concernant le traitement des données utilisateur », *Forbes*, 15 décembre 2020.
20. Propos relayés *in* BENSIMON Cyril et LA CAM Morgane, « Mali : dans la guerre de l'information, l'armée française réplique et accuse le Groupe Wagner », *Le Monde*, 23 avril 2022.

21. Laurent Gbagbo était accusé de quatre chefs de crimes contre l'humanité perpétrés dans le contexte des violences post-électorales en Côte d'Ivoire en 2010-2011. L'ancien président ivoirien a finalement été acquitté de tous les chefs d'accusation par la Chambre de 1re instance de la CPI en 2019. Pour plus d'informations sur cette affaire, voir la fiche d'information sur l'affaire Gbagbo et Blé Goudé établie par la CPI.
22. CPI, Chambre préliminaire I, *Décision portant ajournement de l'audience de confirmation des charges conformément à l'article 61-7-c-i du Statut*, n° ICC-02/11-01/11-432, 3 juin 2013, § 29, p. 13.
23. Haut-Commissariat des Nations unies aux Droits de l'Homme, *loc. cit.*
24. *Ibid*.
25. International Bar Association, « EyeWitness to Atrocities app reaches 10,000 milestone of verifiable photos and videos relating to war in Ukraine », 13 mai 2022.
26. AL-HLOU Yousur, FROLIAK Masha, HILL Evan, BROWNE Malachy et BOTTI David, « New evidence shows how Russian soldiers executed men in Bucha », *New York Times*, 19 mai 2022.
27. Sky News, « Ukraine war: full interview with Putin's spokesman », sur Youtube, mise en ligne le 7 avril 2022.
28. Site web War on Fakes.
29. Amnesty International, « Ukraine: Ukrainian fighting tactics endanger civilians », 4 août 2022.
30. Amnesty International, « Statement on publication of press release on Ukrainian fighting tactics », 7 août 2022.
31. Pour plus d'informations sur ce principe, voir OSCE, *Recueil juridique des standards internationaux relatifs à un procès équitable*, 2013.
32. CPI, Bureau du procureur, Code de conduite du Bureau du procureur, entré en vigueur le 5 septembre 2013, § 49, p. 14.
33. Parmi elles, l'organisation non gouvernementale Fair Trials, organisme mondial de surveillance de la justice pénale, fait campagne pour l'équité, l'égalité et la justice.
34. Voir notamment CPI, Chambre préliminaire I, *loc. cit.*, n° ICC-02/11-01/11-432, 3 juin 2013, § 35, p. 17-18.
35. Voir notamment BAYLIS Elena, « Outsourcing Investigations », *UCLA Journal of International Law and Foreign Affairs*, vol. 14, n° 1, 2019, p. 121-147.
36. En ce qui concerne la CPI voir le Règlement de procédure et de preuve, règles 63-75.