CLINIQUE DOCTORALE
AIX GLOBAL JUSTICE

Clinique de Droit international des droits de l'homme

www.aixglobaljustice.org

Contribution pour l'étude thématique sur les nouvelles technologies et les disparitions forcées

Étude du conflit armé en Ukraine

Février 2023

Ce travail a été réalisé sous la coordination de Nathanael GRIFFART et Jean MAZEL, membres de la Clinique doctorale de droit internationale des droits de l'homme et grâce au concours d'étudiants cliniciens en droit :

Sophie BEROUD
Carla DOGHMAN
Maelle GROSSAIN-CAMIER
Gaëtan LEGRIGEOIS

Ce document est produit à titre d'information et s'inscrit dans le cadre des travaux de la Clinique et d'un partenariat académique. Aix-Marseille Université et l'ensemble de ses composantes déclinent toute responsabilité quant au contenu du document et quant à son utilisation ultérieure.

La dernière mise à jour date du 02 février 2023.

Pour toute question complémentaire sur ce dossier, veuillez contacter :

Nathanaël GRIFFART
nathanael.grf@protonmail.com
+33 768744378

Jean MAZEL
jeanmzl@protonmail.com
+33 626314209

ou

Adeline AUFFRET et Indira BOUTIER, Coordinatrices générales de la Clinique Aix Global Justice :
aixglobaljustice@gmail.com
aixglobaljusticeclinic@proton.me

La Clinique est dirigée par le Professeur Ludovic HENNEBEL et les travaux se font sous sa direction.

Table des matières

Abréviations

CourEDH	Cour européenne des droits de l'homme
Russie	Fédération de Russie
CAI	Conflit armé international
CPI	Cour pénale internationale
DF	Disparitions forcées
DUDH	Déclaration Universelle des droits de l'Homme
DH	Droits de l'Homme
DIH	Droit International Humanitaire
NT	Nouvelles technologies
DP	Données personnelles
IA	Intelligence artificielle
RF	Reconnaissance faciale
PIDCP	Pacte International des Droits Civils et Politiques

Questionnaire relatif à l'étude thématique sur "les nouvelles technologies et les disparitions forcées" du Groupe de travail sur les disparitions forcées ou involontaires

1. **1.1) Pouvez-vous illustrer les principaux risques présentés par l'utilisation des nouvelles technologies par rapport au travail des défenseurs des droits de l'homme et, en particulier, des proches des disparus ? 1.2) Comment ces risques peuvent-ils être atténués ? 1.3) Pouvez-vous donner des exemples concrets de la manière dont les nouvelles technologies ont été utilisées comme un outil pour entraver les familles des personnes disparues et les défenseurs des droits humains dans leur lutte pour la vérité et la justice (y compris par le biais de la cyber-intimidation, du harcèlement sexuel, etc.) ? 1.4) Comment le système judiciaire peut-il offrir une protection efficace contre ce type de harcèlement ?**

2. **Comment pensez-vous que les nouvelles technologies sont utilisées/peuvent être utilisées pour faciliter la commission d'une disparition forcée (par exemple, en traquant d'éventuelles victimes ou en exerçant une surveillance sur leurs proches) et pour dissimuler la commission d'une disparition forcée (si possible, donner des exemples concrets) ?**

3. **3.1) Pouvez-vous illustrer le cadre juridique applicable (réglementations et politiques), le cas échéant, dans votre pays (ou dans les pays de votre intérêt) pour faire face, en particulier, (a) aux coupures ou restrictions d'Internet ? ; (b) cyber-surveillance et attaques, (c) campagnes de désinformation ; et (d) l'utilisation de spyware ?**

6. **Existe-t-il des exemples précis où l'utilisation abusive des nouvelles technologies pour harceler les défenseurs des droits de l'homme, y compris les familles de personnes disparues, ou pour faciliter la commission d'une disparition forcée ou pour la dissimuler, a fait l'objet d'une enquête, de poursuites et la punition des responsables ? Veuillez illustrer les principaux obstacles rencontrés dans ce domaine, ainsi que les leçons apprises et les bonnes pratiques.**

7. **Comment les nouvelles technologies (et quelles nouvelles technologies) peuvent-elles faciliter la recherche de personnes disparues de force (en donnant, si possible, des exemples concrets et en illustrant le fonctionnement de ces technologies) ? Quels sont les outils « indispensables » dans ce domaine ? Ces outils sont-ils facilement accessibles et abordables, ou existe-t-il des obstacles spécifiques à leur achat et à leur utilisation ?**
8. **Quelles sont les nouvelles technologies qui ont donné les résultats les plus significatifs en matière de recherche de personnes disparues de force et comment fonctionnent-ils ? Existe-t-il des différences pratiques significatives dans les technologies qui seront utilisées dans la recherche de la personne décédée ou**

vivante ?

10. **Pouvez-vous indiquer les bonnes pratiques, ainsi que les principaux obstacles (pratiques et juridiques) rencontrés par vous/votre pays (ou dans les pays de votre intérêt) /institution/organisation dans l'utilisation des nouvelles technologies pour enquêter sur les cas de disparition forcée (si possible, en donnant des exemples concrets) ? Quels sont les outils que vous considérez comme les plus efficaces à ces fins ? Ces outils sont-ils facilement accessibles et abordables, ou existe-t-il des obstacles spécifiques à leur achat et à leur utilisation ?**

11. **Quelles sont les « éléments » que vous considérez comme essentiels pour prouver le crime de disparition forcée et qui peuvent être recueillis grâce à l'utilisation des nouvelles technologies ? Voyez-vous des problèmes spécifiques dans la préservation de la chaîne de possession ici et dans l'admissibilité de certaines preuves spécifiques de ce crime recueillies grâce à l'utilisation des nouvelles technologies ?**

La présente contribution porte sur l'étude des disparitions forcées et leur lien avec les nouvelles technologies sur le territoire ukrainien à travers le prisme du conflit russo-ukrainien ayant débuté en 2014. Au sein du conflit russo-ukrainien, les nouvelles technologies n'ont jamais été autant utilisées et instrumentalisées par le pouvoir politique et militaire notamment pour commettre, dissimuler ou mettre fin à une disparition forcée. Ce conflit a pu révéler l'importance des nouvelles technologies au sein des conflits armés contemporains et l'enjeu que représente leur régulation en droit international.

Réponses aux questions

1.1) L'utilisation des nouvelles technologies (NT) par un État dans le cadre d'un conflit armé international (CAI) peut entraver le travail de recherche des personnes disparues et ce, notamment en exposant leurs proches et les défenseurs des droits de l'Homme à des risques **d'espionnage** et de **harcèlement**.

Un État peut espionner une population et ses déplacements[1] en ayant recours à l'intelligence artificielle (IA) combinée à la reconnaissance faciale (RF).

Par ailleurs, les autorités étatiques peuvent user des NT afin d'harceler les proches des disparus ou les défenseurs des droits de l'Homme[2], les empêchant ainsi manifestement de jouir de leurs libertés d'expression[3] ou d'association[4].

1.2) Les risques de harcèlement peuvent être atténués par la régulation du contenu en ligne. Ici, le rôle des réseaux sociaux est primordial. Ils mettent en place des algorithmes visant à prévenir ce type d'abus qui doivent cependant être renforcés. Par ailleurs, les algorithmes mis en place par les administrateurs et opérateurs de plateformes en ligne peuvent s'appuyer sur des considérations économiques et politiques pour faire fi du bien-être des utilisateurs. Dans ce cadre, une régulation et un contrôle judiciaire des algorithmes basés sur la protection des DH s'avèrent nécessaires

S'agissant de l'espionnage, de nombreux textes non contraignants visent à encourager les entreprises à **faire preuve de vigilance** dans la mesure où les outils qu'elles développent sont utilisés pour surveiller la population[5]. Les entreprises se doivent de prendre des mesures raisonnables afin que leurs activités ne portent pas atteinte aux DH et aux libertés

[1] Comité pour l'élimination de la discrimination raciale, *Recommandation générale no 36 sur la prévention et l'élimination du recours au profilage racial par les représentants de la loi*, CERD/C/GC/36, 2020, p. 9. ici.
[2] Anastasiia Kruope, « In Belarus, jailed for protecting loved ones », *Human rights Watch*, 23 janvier 2023. ici.
[3] Article 19, Pacte international des droits civils et politiques (PIDCP).
[4] Article 12 et article 22, PIDCP.
[5] Directrice de la Division de l'engagement thématique, des procédures spéciales et du droit au développement au Haut-Commissariat, *Le Conseil des droits de l'homme tient un dialogue avec le Rapporteur spécial sur la promotion de la vérité, de la justice, de la réparation et des garanties de non-répétition*, 16 septembre 2022, §11 ici.

fondamentales[6]. Ce devoir de diligence est consacré par l'OCDE[7] mais aussi progressivement par l'Union européenne[8].

1.3) L'utilisation abusive des services de messagerie électronique entrave l'activité d'une défenseuse des droits ukrainienne recevant des intimidations et menaces de viol par courrier électronique[9].

1.4) L'espionnage[10] de la population peut constituer une violation des droits individuels, notamment le droit au respect de la vie privée[11]. Sur ce fondement, le juge doit contrôler les activités des services de renseignement dès lors que sont en cause des technologies intrusives. Ce contrôle doit s'étendre de la phase d'interception jusqu'à la phase d'utilisation, le juge devant apprécier la nécessité, la proportionnalité et la légitimité de l'ingérence de l'État dans la vie privée des individus à chaque étape du processus[12]. Le contrôle judiciaire de l'utilisation des NT permettrait d'atténuer d'une certaine manière les risques d'espionnage en contrôlant l'activité de l'État.

S'agissant du harcèlement en ligne des individus, **les Etats peuvent être condamnés sur le fondement du droit au respect de la vie privée susmentionné et de la liberté d'aller et venir.** La particularité de son caractère digital amène l'État à devoir trouver un équilibre entre la restriction excessive de l'accès à internet et la régulation des contenus pouvant mener au harcèlement.

Ensuite, **l'Etat peut transposer le principe de « devoir de diligence »[13]** susmentionné afin de pouvoir faire condamner les entreprises participant à ces pratiques.

2. La conservation des DP et la RF sont des outils susceptibles de faciliter la commission de DF en permettant d'identifier et de localiser des individus dans les zones de combats[14] ou aux barrages militaires[15].

---

[6] Guide OCDE sur le devoir de diligence pour une conduite des entreprises, 2018. ici.
[7] *Ibid.*
[8] Proposition de directive du Parlement européen et du Conseil sur le devoir de vigilance des entreprises en matière de durabilité et modifiant la directive (UE) 2019/1937. ici.
[9] Rapporteuse spéciale sur la situation des défenseurs et défenseuses des droits humains, *Rapport Au cœur du combat des défenseurs et défenseuses des droits humains contre la corruption*, A/HRC/49/49, 2021, p. 16. ici.
[10] Il convient de distinguer l'espionnage de défenseurs des DH qui est pertinent en l'espèce à celui de la pratique d'espionnage en DIH qui ici ne présente pas un intérêt pour la question.
[11] Article 17 du PIDCP, article 8 de la Convention européenne des droits de l'homme.
[12] CourEDH, Centrum för rättvisa c. Suède, 25 mai 2021, no 35252/08, §264. ici.
[13] Haut Commissariat des Nations Unies au droits de l'Homme, *Résumé du rapport du Groupe de travail sur les entreprises et les droits de l'homme à l'Assemblée Générale des Nations Unies, Diligence raisonnable des entreprises en matière de droits de l'homme: Pratiques émergentes, défis et pistes à suivre*, (A/73/163) octobre 2018. ici.
[14] *UN Human Rights Monitoring Mission in Ukrain*e, *Report on the human rights situation in Ukraine*, *op.cit.*, p.26.
[15] Luc Chagnon, « Guerre en Ukraine : la reconnaissance faciale, un outil controversé pour identifier les soldats russes morts au combat », *Franceinfo*, 4 juillet 2022. ici.

Le récolte d'opinions en ligne et le traitement de DP grâce à des logiciels de surveillance (e.g. **Angel.Destruktiv**[16]**, le SBU**[17]) pourraient également faciliter l'identification des opposants.

3.1) Les Constitutions russes et ukrainiennes, bien que garantissant la liberté d'expression et la liberté de recevoir et diffuser des informations[18], **ne font pas mention d'Internet** et ce, alors que les restrictions s'intensifient depuis le commencement du CAI.

Pour lutter contre les cyberattaques, un **Centre national de coordination pour la cybersécurité**[19] et un **système de protection de l'information de bout en bout**[20], empêchant les tiers d'accéder aux informations[21], ont été créés en Ukraine. Eu égard à la coordination internationale en la matière, l'Estonie et l'Angleterre ont fourni du matériel et des logiciels de pointe pour enquêter sur les cybercrimes[22].

Parallèlement, la Russie développe une stratégie pour **contrer les cyberattaques**[23] **grâce à la construction du RuNet**, lequel est en cours de perfectionnement et devrait permettre de fermer les accès Internet menant à la Russie en continuant de conserver les services essentiels du réseau.

Le code pénal ukrainien prévoit également des **infractions en matière de cybersécurité**[24]. Enfin, une subdivision du service d'État des communications spéciales et de la protection de l'information assure la **protection des systèmes de télécommunication de l'État** et réagit aux **incidents de sécurité informatique**.

Par ailleurs, dans le contexte du CAI, le DIH est le droit applicable, la législation ukrainienne relative aux cyberattaques n'a pas forcément vocation à s'appliquer. Le DIH n'interdit pas les cyberattaques **à condition que celles-ci respectent les principes régissant la conduite des hostilités**, notamment **les principe de précaution, de distinction et de proportionnalité**[25]. Ces principes s'appliquent en particulier **aux cyberoutils qui ont été conçus pour s'auto-propager et affecter sans discrimination des systèmes informatiques utilisés à grande échelle**[26]. L'enjeu actuel lié aux cyberattaques dans le cadre d'un conflit armé est d'admettre

---

[16] « Russia develops tech for monitoring deviant behavior », *Moscow Times*, 5 octobre 2021. ici.
[17] « Ukraine la situation des droits humains en 2021 », Amnesty International, 2021. ici.
[18] Article 29, Constitution russe de 1993. Article 34, Constitution ukrainienne de 1996.
[19] Décret du président ukrainien n° 96/2016 sur la stratégie de cybersécurité de l'Ukraine du 15 mars 2016.
[20] Loi n° 2163-VIII sur les principes fondamentaux de la cybersécurité de l'Ukraine du 5 octobre 2017.
[21] Résolution du Cabinet des ministres n°518 sur l'adoption des exigences générales en matière de cybersécurité des objets d'infrastructures critiques du 19 juin 2019.
[22] Cybersecurity in Ukraine: National Strategy and international cooperation, *Global Forum on Cyber Expertise*, 7 juin 2017. ici.
[23] Loi sur la création d'un Internet souverain, 16 avril 2019 ; Loi n°608767-7, 1er mai 2019 pour un Internet sûr et durable.
[24] Articles 360 à 363.
[25] Article 48, Protocole Additionnel I aux Conventions de Genève. Règles 1,7, 14 et 22 du Comité international de la croix rouge (CICR), Étude sur le DIH coutumier ; CIJ, *Licéité de la menace ou de l'emploi d'armes nucléaires*, § 78.
[26] « Le droit international humanitaire et les cyberopérations pendant les conflits armés - Position du CICR », *op. cit.*

que **leur utilisation à l'encontre des infrastructures comme les hôpitaux ou les infrastructures énergétiques, peut constituer un crime de guerre**. Le procureur de la CPI a été saisi de cette question par l'Ukraine à la suite de multiples cyberattaques sur le territoire ukrainien par la Russie[27].

Le cadre juridique russe relatif à la désinformation a, lui, été modifié trois fois entre 2016 et 2022. Les **plateformes sont devenues responsables de la véracité des informations publiées,** et le **pouvoir du Roskomnadzor**[28] **a été renforcé**, ce dernier pouvant ordonner la qualification d'une information de *fake news*[29]*,* **sans décision de justice préalable**[30]. Ensuite, **des amendements pénalisant la discréditation des forces armées nationales ont été votés**[31]. L'imprécision des législations et la manipulation de l'information par les pouvoirs publics permettent aux États et aux agents publics de pratiquer la diffusion de la désinformation et notamment dans le cadre d'un conflit armé[32]. De plus, la législation russe en cause peut être instrumentalisée dans l'objectif de réduire au silence les principaux opposants au régime, comme c'est le cas des lois sur la sécurité nationale[33]. Le contrôle de l'information par les pouvoirs publics tend également à réduire la communication entre les individus dans le cadre d'un conflit armé et donc à les mettre potentiellement en danger du fait de leur incapacité à évaluer les risques pour leur sécurité sur le territoire[34]. **La réduction des communications entre les individus facilite la commission de DF tout en entravant leurs enquêtes.**

En Ukraine, la doctrine de la sécurité informationnelle ne fait aucune référence à la désinformation contrairement à la propagande et les informations non fiables qui sont identifiées comme des phénomènes similaires et à endiguer, sans être définies pour autant[35].

6. La poursuite des responsables de l'utilisation abusive des NT facilitant la commission ou la dissimulation d'une DF est presque inexistante dans les deux États, notamment en raison du problème d'indépendance de la justice en Russie[36]et du manque d'information en la

[27] « Ukraine : les cyberattaques russes bientôt devant la CPI », *Futura Sciences.* ici.

[28] Le Service fédéral de supervision des communications, des technologies de l'information et des médias de masse.

[29] Selon l'UNESCO et le Conseil de l'Europe la *fake news* englobe : la désinformation (informations fausses et délibérément créées pour nuire à une personne), la mésinformation (informations fausses créées sans l'intention de nuire) et la mal information (informations basées sur la réalité, utilisées pour infliger un préjudices).

[30]« Comment la Russie peut-elle lutter contre les fausses informations ? », *Observatoire européen de l'audiovisuel*, 19 septembre 2019. ici.

[31] La législation prévoit des peines d'emprisonnement allant de 5 à 10 ans.

[32] Rapporteuse spéciale sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Rapport sur la désinformation et la liberté d'expression pendant les conflits armés, A/77/288, 2022, §60. ici.

[33] *Ibid.*, §4, §61.

[34] *Ibid.*, §21, §102.

[35] Denys Kolesnyk, « L'Ukraine s'apprête à adopter une législation contre la désinformation », *Denys Kolesnyk*, 28 janvier 2020. ici.

[36] Comité des droits de l'Homme, *Rapport Le Comité des droits de l'homme examine le rapport de la Fédération de Russie en l'absence de délégation et s'inquiète des graves violations des droits de l'homme rapportées tant dans le pays que dans le cadre de l'agression contre l'Ukraine*, 20 octobre 2022. ici.

matière en Ukraine. Par ailleurs, le Groupe de travail sur les DF affirme **qu'aucune affaire concernant des auteurs de DF n'a été portée devant la justice ukrainienne** en 2019[37].

7. Les images satellites, la création de banque de données ADN et le *crowdsourcing* facilitent la recherche de personnes disparues. Lors du massacre de Boutcha, les images satellites de la société Maxar Technologies ont permis de localiser et identifier des corps, facilitant la recherche de personnes disparues[38].

Ensuite, la méthode du *crowdsourcing* permet de récolter des renseignements fournis par la population signalant une DF.

Cependant, **ces outils sont coûteux et sont pour la plupart sous le contrôle des grandes puissances occidentales tels que les États-Unis, dépendant donc de leur coopération**.

8. Les NT relatives aux **bases de données génétiques et les logiciels de RF donnent des résultats significatifs** en comparant les profils ADN de membres d'une famille avec celui d'un cadavre non identifié ou de restes humains[39]. A cette fin, la recherche en parentalité et la création de bases de données génétiques centralisées comme "I-Familia"[40] d'INTERPOL, améliorent l'identification de personnes disparues[41].

D'un point de vue pratique, ces deux technologies peuvent être utilisées **aussi bien dans la recherche des personnes décédées que vivantes.**

10. Lors d'enquête de DF, **l'Ukraine utilise la RF afin d'identifier les personnes décédées sur le front**[42].

Toutefois, recourir à ce système intrusif basé sur l'IA affecte de nombreux DH en ce qu'**il représente une immixtion au droit à la vie privée et un risque à la protection des DP**.

En effet, l'atteinte à la vie privée doit être légitime, nécessaire et proportionnée. Or, ces NT peuvent être utilisées pour organiser une surveillance de masse, agissant de manière indiscriminée et disproportionnée.

De plus, des études ont révélé que les IA et RF reconnaissent plus facilement les hommes blancs que les femmes ou que les autres groupes ethniques. Ainsi, la NT utilisée dans le cadre d'une enquête peut induire en erreur concernant l'identification du coupable, et plus

---

[37] Groupe de travail sur les disparitions forcées ou involontaires, *Visite en Ukraine*, A/HRC/42/40/Add.2, 9 août 2019. ici.

[38] « Massacre de Boutcha en Ukraine : des images satellite et des observations sur le terrain pointent la responsabilité des soldats russes », *France TV Info*, avril 2022. ici.

[39] « INTERPOL présente une nouvelle base de données mondiale d'identification des personnes disparues grâce à l'ADN familial », *INTERPOL*, 1 juin 2021. ici.

[40] « Identification au niveau mondial de personnes disparues par la recherche ADN en parentalité », *INTERPOL*, 1 juin 2021. ici.

[41] Document thématique « Personnes disparues et victimes de disparition forcée en Europe », *Commissaire aux droits de l'homme du Conseil de l'Europe*, 2016. ici.

[42] « Ukraine has started using Clearview AI's facial recognition during war », *Reuters*, 14 mars 2022. ici.

particulièrement lorsqu'il s'agit de personne de couleur, ou de femmes[43], portant atteinte au principe de non discrimination[44].

11. Les éléments essentiels pour prouver le crime de DF via les NT sont les **images, données, identification des individus et le crowdsourcing.** Dans le contexte du conflit Russo-Ukrainien, le Congrès américain a d'ailleurs demandé aux plateformes web de **conserver les téléchargements** afin de recueillir des preuves de violations des DH[45].

Ensuite, **un système de *blockchain,*** tel que "I-Familia", permet le stockage et l'échange d'informations de manière ultra-sécurisée, évitant toute immixtion[46].

Néanmoins, ce type de système et de conservation de DP[47] peut poser des problèmes spécifiques. **La conservation des données par certaines plateformes augmente le risque de piratage de celles-ci, et donc, de détournement**. A ce sujet, la CourEDH a estimé que la durée de conservation d'empreintes génétiques récoltées par la police dans le cadre d'une infraction devait être d'une part, proportionnelle à la nature ou gravité de celle-ci, et d'autre part, déterminée en fonction de la finalité de sa conservation[48] sous peine de porter atteinte au droit à la vie privée du requérant. Cependant, cet arrêt a été rendu en temps de paix et **ne traite donc pas des dérogations susceptibles d'opérer en temps de conflit armé** et pouvant avoir pour effet de rendre ces pratiques licites[49] selon le principe de la *lex specialis derogat legi generali*.

[43] Steve Lohr, « Facial Recognition Is Accurate, if You're a White Guy», *New York Times,* 9 février 2018.
[44] Article 2 de la DUDH.
[45] Mathilde Rochefort, « Les réseaux sociaux sommés de conserver les images de crimes de guerre par le Congrès », *Siècle Digital*, 13 mai 2022. ici.
[46] « Identification au niveau mondial de personnes disparues par la recherche ADN en parentalité », *INTERPOL, op. cit.*
[47] Fiche thématique "Protection des données personnelles", Service de l'exécution des arrêts de la Cour européenne des droits de l'homme, DG1, Conseil de l'Europe, septembre 2022. ici.
[48] CourEDH, *Aycaguer c. France,* 22 juin 2017, req. n°8806/12.
[49] Article 4 du PIDCP. ici.

Bibliographie

LÉGISLATIONS

- *Droit ukrainien*

Constitution ukrainienne.

Décret du président ukrainien n° 96/2016 sur la stratégie de cybersécurité de l'Ukraine du 15 mars 2016.

Loi n° 2163-VIII sur les principes fondamentaux de la cybersécurité de l'Ukraine du 5 octobre 2017.

Résolution du Cabinet des ministres n°518 sur l'adoption des exigences générales en matière de cybersécurité des objets d'infrastructures critiques du 19 juin 2019.

- *Droit russe*

Constitution russe.

Loi sur la création d'un Internet souverain du 16 avril 2019.

Loi n°608767-7 du 1er mai 2019 pour un Internet sûr et durable.

CONVENTIONS ET INSTRUMENTS INTERNATIONAUX

Convention européenne des droits de l'homme, 4 novembre 1950.

Convention internationale pour la protection de toutes les personnes contre les disparitions forcées, 20 décembre 2006.

Convention 108 pour la protection des données à caractère personnel, 28 janvier 1981.

Convention sur la violence et le harcèlement, 25 juin 2021.

Proposition de directive du Parlement européen et du Conseil sur le devoir de vigilance des entreprises en matière de durabilité et modifiant la directive (UE) 2019/1937.

Déclaration Universelle des Droits de l'Homme.

Pacte international des droits civils et politiques.

Protocole Additionnel I aux Conventions de Genève.

Guide OCDE sur le devoir de diligence pour une conduite des entreprises, 2018.

JURISPRUDENCES

Cour Internationale de Justice, avis consultatif, *Licéité de la menace ou de l'emploi d'armes nucléaires,* 8 juillet 1996.

Cour européenne des droits de l'homme, *Aslakhanova et autres c. Russie*, 18 décembre 2012, req. n° 2944/06, 332/08, 42509/10 et al.

Cour européenne des droits de l'homme, *Aycaguer c. France*, 22 juin 2017, req. n°8806/12

Cour européenne des droits de l'homme, *Centrum för rättvisa c. Suède*, 25 mai 2021, req. n°35252/08, §264.

Cour européenne des droits de l'homme (Grande Chambre), *Ukraine c. Russie (Crimée)*, 16 décembre 2020, req. n° 20958/14 et 38334/18, §186.

Cour européenne des droits de l'homme, *Rotaru c. Roumanie*, 4 mai 2000, req. n°28341/95

OUVRAGES

Wolfgang Benedek, et Matthias C. Kettemann. « Exemples de pratiques au niveau national », *Liberté d'expression et internet,* sous la direction de Benedek Wolfgang, Matthias C. Kettemann, Conseil de l'Europe, 2014, pp. 107-125.

ARTICLES

Fabien Lafouasse, « L'espionnage en droit international, Annuaire français de droit international, 2001, p.127. »

Francesca Musiani, Benjamin Loveluck, Françoise Daucé, Ksenia Ermoshina, « Souveraineté numérique : l'Internet russe peut-il se couper du reste du monde ? », HAL, 2019.

ARTICLES DE PRESSE

Anastasiia Kruope, « In Belarus, jailed for protecting loved ones », *Human rights Watch*, 23 janvier 2023. Consulté le 2 février 2023.

Benoit Viktine, « La Russie va rendre publiques les adresses personnelles des "agents de l'étranger" », *Le Monde*, 14 novembre 2022. Consulté le 2 février 2023.

Cybersecurity in Ukraine: National Strategy and international cooperation, *Global Forum on Cyber Expertise*, 7 juin 2017. Consulté le 2 février 2023.

Luc Chagnon, « Guerre en Ukraine : la reconnaissance faciale, un outil controversé pour identifier les soldats russes morts au combat », *Franceinfo*, juillet 2022. Consulté le 2 février 2023.

Mathilde Rochefort, « Les réseaux sociaux sommés de conserver les images de crimes de guerre par le Congrès », *Siècle Digital*, 13 mai 2022. Consulté le 2 février 2023.

Michael Cooney, « Bien que malmené, l'Internet ukrainien résiste », *Le Monde Informatique*, 7 mars 2022. Consulté le 2 février 2023.

« Massacre de Boutcha en Ukraine : des images satellite et des observations sur le terrain pointent la responsabilité des soldats russes », *France TV Info*, avril 2022. Consulté le 2 février 2023.

« Près de la ville assiégée de Marioupol, des images satellite révèlent des “fosses communes” », *Le Monde*, avril 2022. Consulté le 2 février 2023.

« Russia bans smartphones for soldiers over social media fears », *BBC News*, 20 February 2019. Consulté le 2 février 2023.

« Russia develops tech for monitoring ”deviant behavior », *Moscow Times*, 5 octobre 2021. Consulté le 2 février 2023.

Steve Lohr, « Facial Recognition Is Accurate, if You’re a White Guy», *New York Times*, 9 février 2018. Consulté le 2 février 2023.

« Ukraine has started using Clearview AI’s facial recognition during war », *Reuters*, 14 mars 2022. Consulté le 2 février 2023.

« Un logiciel de surveillance russe se retourne contre le Kremlin », *Watson*, 6 mai 2022. Consulté le 2 février 2023.

« Putin bans VPNs to stop Russians accessing prohibited websites », *Reuters*, 30 juillet 2017. Consulté le 2 février 2023.

RAPPORTS

- *Rapports d’organisations internationales*

Commissaire aux droits de l’homme du Conseil de l’Europe, *Document thématique Personnes disparues et victimes de disparition forcée en Europe*, 2016.

Comité des droits de l’homme, Office des Nations Unies à Genève, *Examen du rapport de l’Ukraine : le Comité des droits de l’homme insiste sur l’importance de la liberté d’expression et de l’indépendance de la justice*, 26 octobre 2021.

INTERPOL, *Identification au niveau mondial de personnes disparues par la recherche ADN en parentalité,* 1 juin 2021.

Comité des droits de l'homme, Office des Nations Unies à Genève, *Le Comité des droits de l'homme examine le rapport de la Fédération de Russie en l'absence de délégation et s'inquiète des graves violations des droits de l'homme rapportées tant dans le pays que dans le cadre de l'agression contre l'Ukraine,* 20 octobre 2022.

Rapporteuse spéciale sur la situation des défenseurs et défenseuses des droits humains, *Rapport Au cœur du combat des défenseurs et défenseuses des droits humains contre la corruption*, A/HRC/49/49, 2021, p. 16.

Groupe de travail sur les détentions arbitraires, notamment la question de la torture et de la détention, *Rapport sur les droits civils et politiques*, E/CN.4/2006/7, 2005, p.16.

Rapporteuse spéciale sur la situation des défenseurs et défenseuses des droits humains, *Rapport sur l'Ultime mise en garde contre les menaces de mort reçues par les défenseurs et défenseuses des droits humains et contre les exécutions dont ils font l'objet*, A/HRC/46/35, 2020, p. 6.

Comité pour l'élimination de la discrimination raciale, *Recommandation générale no 36 sur la prévention et l'élimination du recours au profilage racial par les représentants de la loi*, CERD/C/GC/36, 2020, p. 9.

Service de l'exécution des arrêts de la Cour européenne des droits de l'homme, DG1, Fiche thématique "Protection des données personnelles", Conseil de l'Europe, septembre 2022.

UN Human Rights Monitoring Mission in Ukraine, *Report on the human rights situation in Ukraine*, 27 septembre 2022.

Groupe de travail sur les disparitions forcées ou involontaires, *Visite en Ukraine*, A/HRC/42/40/Add.2, 9 août 2019.

Rapporteuse spéciale sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Rapport sur la désinformation et la liberté d'expression pendant les conflits armés, A/77/288, 2022.

Directrice de la Division de l'engagement thématique, des procédures spéciales et du droit au développement au Haut-Commissariat, *Le Conseil des droits de l'homme tient un dialogue avec le Rapporteur spécial sur la promotion de la vérité, de la justice, de la réparation et des garanties de non-répétition*, 16 septembre 2022.

- *Rapports d'organisations non-gouvernementales*

« Russie : Des civils ukrainiens victimes de disparitions forcées », *Human Rights Watch*, 14 juillet 2022.

« Ukraine la situation des droits humains en 2021 », *Amnesty International*, 2021.

« Le droit international humanitaire et les cyberopérations pendant les conflits armés - Position du CICR », *Comité international de la Croix Rouge*, novembre 2019.

Haut Commissariat des Nations Unies au droits de l'Homme, *Résumé du rapport du Groupe de travail sur les entreprises et les droits de l'homme à l'Assemblée Générale des Nations Unies, Diligence raisonnable des entreprises en matière de droits de l'homme: Pratiques émergentes, défis et pistes à suivre,* (A/73/163) octobre 2018.

- *Communiqués et déclarations*

« Comment la Russie peut-elle lutter contre les fausses informations ? », Observatoire européen de l'audiovisuel, 19 septembre 2019.

Communication publique n°3760 de la Fédération de Russie, 9 septembre 2022.

Communiqué du Rapporteur spécial sur la situation des défenseurs des droits de l'homme, le Groupe de travail sur les détentions arbitraires, le Groupe de travail sur les disparitions forcées ou involontaires, le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, le Rapporteur sur la promotion et la protection des droits et libertés fondamentaux dans la lutte contre le terrorisme, AL RUS 10/2022, 30 octobre 2022.

Conseil de l'UE, Règles sur le devoir de vigilance pour les grandes entreprises : le Conseil adopte sa position, 1 décembre 2022.

« Déclaration à l'occasion de la Journée internationale des victimes de disparition forcée », *Conseil de l'Europe*, 28 août 2022.

« Le Comité des droits de l'homme examine le rapport de la Fédération de Russie en l'absence de délégation et s'inquiète des graves violations des droits de l'homme rapportées tant dans le pays que dans le cadre de l'agression contre l'Ukraine », *Nations Unies*, 20 octobre 2022.

« Le Conseil des droits de l'homme tient un dialogue avec le Rapporteur spécial sur la promotion de la vérité, de la justice, de la réparation et des garanties de non-répétition », Directrice de la Division de l'engagement thématique, des procédures spéciales et du droit au développement au Haut-Commissariat, 16 septembre 2022.

« *Joint declaration on freedom of expression and "fake news", disinformation and propaganda, organization of american states* », Haut-Commissariat aux droits de l'homme, OSCE, Union africaine, 3 mars 2017.

SITES INTERNET

Cyril Cléaud, « Alerte sécurité HermeticWiper & CaddyWiper : la réponse des produits Stormshield », *Stormshield*, 25 février 2022. Consulté le 2 février 2023.

Denys Kolesnyk, « L'Ukraine s'apprête à adopter une législation contre la désinformation », *Denys Kolesnyk*, 28 janvier 2020. Consulté le 2 février 2023.

« INTERPOL présente une nouvelle base de données mondiale d'identification des personnes disparues grâce à l'ADN familial », INTERPOL, 1er juin 2021. Consulté le 2 février 2023.

« *Ukraine Conflict: Cyberattacks, Frequently Asked Questions* », *Cyber Peace Institute*, 16 juin 2022. Consulté le 2 février 2023.

« Ukraine : les cyberattaques russes bientôt devant la CPI », *Futura Sciences*. Consulté le 2 février 2023.