

Une « diplomatie des données par le bas » : la défense des droits humains en contexte d'autoritarisme numérique

Article inédit, mis en ligne le 23 septembre 2026

Julien Hocine

Julien Hocine est doctorant en communication à l'Université du Québec à Montréal, assistant de recherche à la Chaire de recherche du Canada en éducation aux médias et droits humains et chargé de cours. Ses travaux de recherche portent sur les usages des technologies, les imaginaires sociotechniques, et les représentations du Nord et de l'Arctique.

Hocine.julien@courrier.uqam.ca

Julia Bihl

Julia Bihl est docteure en sciences de l'information et de la communication, collaboratrice du GReMS et chargée de cours à l'Université catholique de Louvain (Belgique). Ses travaux de recherche portent sur l'éducation aux médias, la littératie médiatique, la pensée critique et l'émancipation sociale.

Julia.bihl@uclouvain.be

Normand Landry

Normand Landry est professeur titulaire à l'Université TÉLUQ. Il est également titulaire de la Chaire de recherche du Canada en éducation aux médias et droits humains. Ses travaux se concentrent sur l'éducation aux médias, les droits de la communication, l'intimidation judiciaire, les représentations de la pauvreté, ainsi que sur la communication et les mouvements sociaux.

Normand.landry@teluq.ca

Simon Fitzbay

Simon Fitzbay est étudiant au doctorat à l'Université du Québec à Montréal et assistant de recherche à la Chaire de recherche du Canada en éducation aux médias et droits humains. Ses travaux de recherche portent sur le rôle de la technique dans le domaine de l'éducation dans une perspective d'économie politique.

fitzbay.simon@courrier.uqam.ca

Marie-Josée Dupuis

Marie-Josée Dupuis est professionnelle de recherche à la Chaire de recherche du Canada en éducation aux médias et droits humains. Ses travaux de recherche portent sur la pauvreté et les inégalités, la précarisation du marché du travail et les mouvements sociaux.

marie-josée.dupuis@teluq.ca

Plan de l'article

Introduction

Penser la gouvernance des données depuis les marges

Modalités d'analyse de la revue de littérature

Les catégories de répression numérique : surveillance, censure et propagande

Les catégories de contraintes sociotechniques

Des tactiques de résistance face à la mise en armement des données numériques

Discussion : Vers une diplomatie des données par le bas

Conclusion

Références bibliographiques

RÉSUMÉ

Dans un contexte marqué par la montée d'un autoritarisme numérique qui instrumentalise les données à des fins de surveillance, de censure et de propagande, cet article analyse les pratiques numériques des défenseur·es des droits humains. Fondé sur une revue systématique de 111 articles savants, il fait la démonstration que ces pratiques constituent une production normative implicite qui conteste les modèles étatiques de gouvernance des données. De fait, elles sont conceptualisées comme une « diplomatie des données par le bas » qui rompt avec une vision de la diplomatie comme une prérogative exclusivement étatique ou technocratique et vise à établir de nouvelles normes pour une circulation plus juste et sécurisée des données sensibles.

Mots clés

Droits humains, activisme numérique, répression numérique, mise en données, gouvernance des données, diplomatie des données.

Title

A Bottom-Up Data Diplomacy : Defending Human Rights in the Context of Digital Authoritarianism.

Abstract

In a context marked by the rise of digital authoritarianism that instrumentalizes data for surveillance, censorship, and propaganda, this article analyzes the digital practices of human rights defenders. Based on a systematic review of 111 scholarly articles, it demonstrates that these practices constitute an implicit normative production that challenges state-centric models of data governance. Indeed, they are conceptualized as a "bottom-up data diplomacy" that breaks with a vision of diplomacy as an exclusively state-based or technocratic prerogative and aims to establish new standards for a fairer and more secure circulation of sensitive data.

Keywords

Human Rights, Digital Activism, Digital Repression, Datafication, Data Governance, Data Diplomacy.

TITULO

Una diplomacia de datos desde abajo: La defensa de los derechos humanos en el contexto del autoritarismo digital.

Resumen

En un contexto marcado por el auge de un autoritarismo digital que instrumentaliza los datos para la vigilancia, la censura y la propaganda, este artículo analiza las prácticas digitales de los defensores de los derechos humanos. Basado en una revisión sistemática de 111 artículos académicos, demuestra que estas prácticas constituyen una producción normativa implícita que desafía los modelos estatales de gobernanza de datos. De hecho, se conceptualizan como una "diplomacia de datos desde abajo" que rompe con una visión de la diplomacia como una prerrogativa exclusivamente estatal o tecnocrática y busca establecer nuevas normas para una circulación más justa y segura de los datos sensibles.

Palabras clave

Derechos Humanos, activismo digital, represión digital, dataficación, gobernanza de datos, diplomacia de datos.

INTRODUCTION

Si elles ont un temps été considérées comme des vecteurs d'émancipation citoyenne, les techniques numériques se sont progressivement imposées comme des instruments centraux de contrôle politique et de répression. Les États exploitent désormais largement le potentiel des infrastructures numériques pour anticiper, surveiller et neutraliser les mobilisations collectives (Dragu et Lupu, 2021), renversant la promesse initiale d'un Internet libérateur (Diamond, 2010 ; Morozov, 2011). Cette dynamique, que *Freedom House* qualifie d'« autoritarisme numérique¹ » (Shahbaz, 2018), s'incarne dans des processus d'instrumentalisation des données à des fins de surveillance, de censure et de propagande. Parallèlement, les principales plateformes numériques privées structurent toujours plus fortement l'accès à l'information et la visibilité des discours publics, et accentuent les asymétries de pouvoir entre producteurs de données, diffuseurs et audiences (Zuboff, 2019; Gregory, 2023).

Les défenseur·es des droits humains se trouvent fréquemment positionnés en première ligne du fait de leurs activités, souvent menées dans des environnements hautement répressifs, qui visent à documenter les violations des droits fondamentaux, en imputer la responsabilité, et protéger les populations ciblées (Assemblée générale des Nations Unies, 1999 ; Land et Aronson, 2020 ; Nah et al., 2013). Face à la mise en données généralisée de leurs actions, les défenseur·es des droits humains développent des stratégies d'adaptation combinant expertise technique, prudence tactique et créativité politique (Landry *et al.*, 2025). Ces pratiques produisent, dans les faits, une contestation implicite des modèles dominants de gouvernance des données, fondés sur la centralisation, l'opacité et l'exclusion des voix dissidentes.

Cet article fait la démonstration que les pratiques numériques des défenseur·es des droits humains esquissent, en creux, une manière alternative d'envisager la régulation des données sensibles, à rebours des logiques de surveillance et de contrôle. En s'appuyant sur une revue de littérature systématique de 111 articles scientifiques en langue anglaise, nous avons dressé un état des lieux des pratiques numériques des défenseur·es des droits humains, des formes actuelles de répression numérique, et des contraintes sociotechniques² qui en découlent.

Nous mobilisons la notion de « diplomatie des données » comme cadre interprétatif pour ces pratiques, celles-ci étant comprises comme des contributions politiques à la reconfiguration des normes encadrant la régulation des données. La notion de « diplomatie des données », telle que proposée par Andrew Boyd *et al.* (2019), désigne l'intervention d'une diversité d'acteurs, au-delà des seuls représentants étatiques, dans les négociations visant à promouvoir l'accès et l'usage des données. Tout en nous inscrivant dans cette perspective qui reconnaît le rôle des acteurs non-étatiques, notre démarche la prolonge en y intégrant une dimension critique et une analyse des rapports de pouvoir. Nous concevons la diplomatie des données non seulement comme un espace de coopération, mais également comme un champ de tensions où les défenseur·es des droits humains, par leurs pratiques en contexte répressif, élaborent « par le bas » une contestation des modèles de gouvernance dominants. La discussion met ainsi en évidence trois formes de diplomatie des données susceptibles de prolonger ces pratiques : une diplomatie pour les données, une diplomatie par les données, et une diplomatie des données partagée.

PENSER LA GOUVERNANCE DES DONNÉES DEPUIS LES MARGES

L'expression « défenseur·e·s des droits humains » intègre des tensions et des ambiguïtés (voir Nah *et al.*, 2013). Formellement, elle désigne « toute personne qui, individuellement ou avec d'autres, agit à des fins de protection et de réalisation des droits humains, tant au niveau national qu'international » (Nations Unies, 1999, art. 12), sans préciser le champ d'action ni le spectre des enjeux couverts.

Trois éléments en balisent les contours. D'abord, la désignation renvoie à des formes de reconnaissance institutionnelle – politiques, juridiques et administratives – qui légitiment des mesures de protection et engagent la responsabilité des acteurs garants de la sécurité des personnes concernées. Ensuite, elle recouvre un ensemble de pratiques inscrites dans des luttes démocratiques non violentes : documentation des violations, assistance aux victimes, mise en imputabilité et promotion de réformes. Enfin, et surtout, elle suppose un cadrage – public, politique et juridique – des activités et des exactions en termes de droits humains. Discursive et performative, elle affirme une adhésion à des normes et des valeurs, et structure des formes d'identification collective. Considérée sous l'angle de la sociologie des mouvements sociaux, elle constitue le « cadre » à l'intérieur duquel se situent et prennent sens les discours et les pratiques d'intervention politique (Benford *et al.*, 2012).

À rebours d'une vision techniciste des données, cet article s'inscrit dans le champ des *Critical Data Studies*, qui conçoivent la donnée comme un objet politique, conflictuel, et situé (Deutch et Al Khatib, 2018). La mise en données (*datafication*) n'est pas un simple processus technique de conversion de l'information, mais un terrain de lutte qui redéfinit les rapports de pouvoir et soulève des enjeux de souveraineté (Nwagwu, 2025 ; Tufekci, 2017). Cette perspective rejoint les travaux francophones en sciences de l'information et de la communication qui, dans le prolongement de l'économie politique du numérique (Mosco, 2016), conçoivent la régulation des données comme un terrain contesté, indissociable des rapports de pouvoir (Bullich et Clavier, 2019). Les travaux récents sur la diplomatie des données soulignent d'ailleurs que les stratégies d'influence se déploient désormais à travers les infrastructures de données elles-mêmes (Lyubareva, Nocetti et Carey-Libbrecht, 2024). Notre démarche prolonge cette filiation en déplaçant l'orientation de l'article vers les acteurs les plus exposés à la répression.

Ce caractère politique de la donnée se manifeste dans l'ambivalence des techniques numériques : mobilisées dans des luttes prodémocratie pour documenter les violations et pour contourner la censure (Costanza-Chock, 2020 ; Lievrouw, 2023 ; Milan, 2013 ; Meikle, 2018 ; McNutt, 2018), elles servent simultanément des stratégies de répression sophistiquées portées par les États et leurs partenaires privés (Deibert, 2015 ; Michaelsen et Glasius, 2018 ; Morozov, 2011 ; Zuboff, 2019 ; Lyon, 2015). Analysés depuis la perspective des acteurs les

plus exposés, les cadres dominants de gouvernance des données – conçus du point de vue étatique ou économique et centrés sur la régulation, la sécurité nationale ou la valorisation commerciale – révèlent leur indifférence aux asymétries de pouvoir qu’ils produisent. La gouvernance doit alors être envisagée non comme un simple ensemble de règles réparties entre acteurs dominants, mais comme un dispositif attentif aux vulnérabilités générées par la mise en données.

L’hypothèse de travail est que, face à un modèle de gouvernance autoritaire qui inverse la « promesse » d’un Internet libérateur (Diamond, 2010 ; Morozov, 2011), les défenseur·es des droits humains développent non seulement de stratégies de résistance et de contournement, mais aussi, implicitement, de nouvelles formes de régulation. Menées sous la contrainte de la répression et des défaillances sociotechniques, leurs pratiques ne constituent pas de simples ajustements techniques : elles esquissent une « diplomatie des données » alternative, construite « par le bas », par et pour les acteurs les plus vulnérables. Distincte de l’activisme numérique, qui mobilise les plateformes pour amplifier des causes (Costanza-Chock, 2020), la diplomatie des données par le bas conteste les règles mêmes des infrastructures de données et désigne la participation d’acteurs non-étatiques à la reconfiguration des normes de gouvernance : qui produit, qui possède, qui légitime et qui archive les données.

Cette tension entre l’instrumentalisation autoritaire des données et leur réappropriation militante invite à formuler une question de recherche centrale : dans quelle mesure les pratiques numériques des défenseur·es des droits humains, déployées sous contrainte répressive, contribuent-elles à reconfigurer les normes de gouvernance des données au-delà des arènes diplomatiques formelles ? Nous considérons ainsi ces pratiques non comme de simples tactiques défensives, mais comme une production normative implicite qui déplace les frontières entre acteurs légitimes et acteurs périphériques de la diplomatie des données.

MODALITÉS D’ANALYSE DE LA REVUE DE LITTÉRATURE

Cet article présente les résultats d’une analyse systématique de la littérature anglophone publiée entre 2010 et 2024 sur les pratiques numériques liées à la défense et à la répression des droits humains. La collecte du corpus a été réalisée en deux phases successives :

- Phase 1 (2022-2023, période couverte 2010-2021). Une exploration préliminaire a permis d’identifier les bases de données pertinentes et de tester différentes combinaisons de mots-clés. Huit bases de données ont été retenues³. Ce choix visait une couverture à la fois des publications en sciences juridiques, en sciences humaines et sociales et dans le domaine interdisciplinaire des droits humains. La recherche par mots-clés a reposé sur des combinaisons associant des descripteurs relatifs aux acteurs (« human rights defenders », « human rights activists », « human rights activism ») et des descripteurs relatifs aux technologies (« digital technology/ies », « media technology/ies », « communication technology/ies »), articulés par les opérateurs booléens *AND* et *OR*. Les champs de recherche ont varié selon les fonctionnalités des bases (titre, résumé, mots-clés ou texte intégral). Cette phase a été complétée par une collecte par méthode boule de neige (examen des bibliographies, validation par titre/résumé, arbitrage conjoint) et a permis de retenir 52 articles.

- Phase 2 (2024-2025, période couverte 2022-2024). Les mêmes bases ont été réinterrogées avec des équations élargies, intégrant de nouveaux descripteurs identifiés dans la littérature. Quatre blocs thématiques d’équations booléennes ont été structurés, couvrant respectivement les dimensions des technologies, de la sécurité numérique, de la mobilisation en ligne et de la gouvernance informationnelle⁴. Cette seconde phase a conduit à l’ajout de 59 articles, portant le corpus total à 111 articles.

Parallèlement aux deux phases, six revues spécialisées en droits humains ont fait l’objet

d'un dépouillement intégral pour l'ensemble des numéros disponibles en ligne⁵. Les revues représentées dans le corpus relèvent de plusieurs champs disciplinaires : sciences de l'information et de la communication, sociologie, sciences politiques, relations internationales et études spécifiques sur les droits humains.

Les critères d'inclusion et d'exclusion du corpus sont les suivants :

- Critères d'inclusion : (a) publication dans une revue à comité de lecture ; (b) rédaction en langue anglaise⁶ ; (c) publication entre 2010 et 2024 ; (d) traitement explicite de pratiques numériques dans le contexte de la défense ou de la répression des droits humains (usages concrets ou stratégies délibérées de technologies numériques).

- Critères d'exclusion : (a) monographies et chapitres de livres (corpus restreint aux articles pour garantir l'homogénéité) ; (b) thèses et mémoires ; (c) littérature grise (rapports institutionnels, documents gouvernementaux, rapports d'ONG), considérée comme sources empiriques pour de futures analyses ; (d) contributions exclusivement théoriques sans référence à des pratiques numériques identifiables ; (e) articles portant sur les technologies comme objet de droits humains (ex. : bioéthique, santé numérique) sans lien avec des répertoires de défense ou de répression.

L'ensemble du corpus a été codé et analysé à l'aide du logiciel NVivo selon une démarche inductive et comparative. Le processus de codage itératif à double arbitrage (Locke *et al.*, 2022 ; Cascio *et al.*, 2019) a conduit à l'élaboration d'une grille d'analyse thématique structurée en cinq volets : (1) les catégories de discours académiques sur la contribution des techniques numériques à la défense des droits humains ; (2) les répertoires de pratiques mobilisant ces technologies ; (3) les répertoires de pratiques répressives ; (4) les facteurs intervenant dans le potentiel d'usage ; (5) les transformations de la pratique de défense des droits humains jugées liées à la numérisation du champ.

Deux concepts ont guidé la grille. Celui de « répertoire d'action collective » (Tilly, 1995 ; Tilly et Tarrow, 2015) renvoie aux routines stratégiques et tactiques partagées, disponibles pour les acteurs mobilisés (Landry *et al.*, 2015) ; la notion de « pratique », ancrée dans la sociologie des usages des TIC (Denouël et Granjon, 2011 ; Kane, 2013), désigne des activités organisées, récurrentes et orientées. Leur articulation situe les appropriations de techniques au sein des luttes sociales, comme des choix opérés parmi un éventail d'options. Le poids relatif des catégories a été établi à partir du nombre d'articles distincts les mentionnant.

Catégories	Sous-catégories
Catégories de discours sur les technologies numériques	Émancipateurs Ambivalents Critiques
Défenseur·es des droits humains : répertoires de pratiques	Pratiques communicationnelles externes Pratiques contentieuses Pratiques d'enquête et documentation Pratiques organisationnelles
Répertoires de pratiques répressives	Censure Propagande Surveillance
Catégories de facteurs	Développement des capacités Sécurité numérique Accès aux ressources matérielles et techniques Caractéristiques des technologies médiatiques Environnement politique et régulateur
Catégories de transformations	Nouvelles méthodes centrées sur les données Nouvelles pratiques d'interaction avec les publics

Notre démarche s'apparente à une revue intégrative (Torraco, 2016) : plutôt que d'agréger des résultats statistiquement comparables, elle produit une cartographie conceptuelle d'un champ fragmenté à partir d'une diversité de devis et de terrains. Les 111 articles y sont mobilisés comme des contributions dont la juxtaposition raisonnée fait émerger des régularités et des catégories transversales.

LES CATÉGORIES DE RÉPRESSION NUMÉRIQUE : SURVEILLANCE, CENSURE ET PROPAGANDE

Pour saisir la portée des pratiques de résistance, il faut d'abord caractériser le régime de contraintes dans lequel elles s'inscrivent. La revue dégage trois catégories de répression numérique – surveillance, censure et propagande – qui constituent les manifestations opératoires d'un paradigme de gouvernance des données fondé sur le contrôle et l'asymétrie de pouvoir, et révèlent une logique de « mise en armement » (*Weaponization*) des données.

La surveillance repose sur l'automatisation de l'identification et de l'extraction des données: cyber espionnage des dissidents (Anstis et LaFlèche, 2025 ; Belmonte, 2023 ; Chubb et Roberts Lyer, 2024 ; Eguridu *et al.*, 2024), captation massive et indifférenciée des flux de communication et conservation prolongée (Stevens *et al.*, 2023), reconnaissance faciale appliquée à l'identification des manifestants (Brough et Li, 2013 ; Gregory, 2010 ; Murray *et al.*, 2024), et mise sous pression des entreprises technologiques pour obtenir des renseignements sur les personnes ciblées⁷ (Anstis et Barnett, 2022 ; El Gody, 2022 ; Stevens *et al.*, 2023). Ce phénomène est soutenu par des lois et réglementations mises en place pour légitimer la surveillance de masse, la rétention des données et l'accès en temps réel aux communications numériques (Ilori, 2024 ; Yingyi et Benyera, 2024). S'y ajoutent des capacités d'infiltration destinées à repérer et anticiper les actions des opposants (Chubb et Roberts Lyer, 2024 ; Tenove, 2019).

La censure combine mesures préventives, blocage et filtrage, de la censure algorithmique (Oral, 2024 ; Yingyi et Benyera, 2024) à la coupure totale ou partielle de la connectivité (*Kill-Switch*) visant à désorganiser les mobilisations (Kasm, 2018 ; Kaun et Tréré, 2020 ; Siatitsa, 2020). Elle s'articule à des campagnes de dénigrement et de harcèlement – notamment par *doxing* – destinées à détruire la réputation des défenseur-es et à inciter à la violence (Nissen, 2023 ; Strand et Svensson, 2023 ; Svensson *et al.*, 2024).

La propagande mobilise la falsification des contenus (*Deepfake*, *Shallowfake*) reposant sur l'accès à de grands volumes de données (Gregory, 2019), le recours à l'IA générative pour produire de fausses preuves et attaquer la crédibilité des militant-es (Freeman, 2021 ; Gregory, 2022 ; Teo, 2025 ; Tripathi, 2022), ainsi que l'automatisation par botnets et « armées de trolls » qui saturent l'espace public (Tenove, 2019 ; Wilson, 2022 ; Gregory, 2023). Ces tactiques ne sont pas l'apanage des seuls régimes en place (Bradshaw et Howard, 2019) : ce qui caractérise leur usage autoritaire est moins un monopole que l'asymétrie de moyens et la capacité à conjuguer leviers étatiques et capacités computationnelles privées.

Ces modalités montrent que la donnée n'est pas un instrument de contrôle passif, mais l'objet d'une instrumentalisation offensive : le passage de la collecte (surveillance) à l'usage délibéré pour nuire, diffamer et neutraliser – campagnes de *hack-and-leak*, incitation à l'autocensure – incarne précisément la « mise en armement » des données numériques (Anstis, 2024 ; Eguridu *et al.*, 2024 ; Gregory, 2019, 2022 ; Oral, 2024).

LES CATÉGORIES DE CONTRAINTES SOCIOTECHNIQUES

Si les pratiques de surveillance, de censure et de propagande constituent les manifestations tangibles de la répression numérique, leur portée et leur efficacité sont exacerbées par les caractéristiques mêmes de l'écosystème numérique dans et à partir duquel elles se

déploient. L'agentivité des défenseur·es des droits humains est en effet doublement contrainte : non seulement par l'action coercitive directe de leurs adversaires, mais également par un ensemble de vulnérabilités qui affectent leur capacité d'action. Les analyses qui suivent soulignent que ces contraintes se déploient sur plusieurs plans : une dimension matérielle, marquée par une inégalité d'accès aux ressources techniques ; une dimension normative, où l'irrecevabilité juridique de leurs données probantes est constante ; et une dimension infrastructurelle, qui les place en situation de dépendance critique envers des infrastructures contrôlées par des acteurs étatiques ou commerciaux. Cette précarité est exacerbée par un déficit à la fois symbolique, à travers la faible reconnaissance de la légitimité de leurs données et des récits qu'ils élaborent, et politique, illustrée par la faiblesse des mécanismes de soutien diplomatique et de recours internationaux.

Les écrits recensés font état de cinq catégories interdépendantes comprenant : (1) des limitations matérielles et techniques, qui instaurent une fracture de moyens et un accès inégal aux données ; (2) des limitations liées au renforcement des capacités, qui révèlent un déficit de littératie et de ressources pour s'adapter à l'environnement numérique ; (3) des limitations liées à la sécurité numérique, qui exposent de manière disproportionnée les militants à des risques constants ; (4) des limitations imposées par l'environnement médiatique, dont la gouvernance algorithmique et la dépendance aux plateformes commerciales façonnent la visibilité des discours, et enfin : (5) des limitations de l'environnement politique et des cadres réglementaires, qui tendent à criminaliser l'action militante plutôt qu'à la protéger.

Tout d'abord, les limitations d'ordre matériel et technique concernent à la fois les inégalités d'accès aux réseaux (connexion internet déficiente ou inexistante dans certains territoires) et aux infrastructures nécessaires pour traiter des données spécifiques et stratégiques, en valider l'authenticité, les stocker et les analyser (Deutch et Al Khatib, 2018 ; Markland, 2021). La littérature souligne un accès limité à l'imagerie satellite (Herscher, 2014 ; Murray *et al.*, 2022) pour documenter des violations à grande échelle et dans des régions non accessibles (déforestation, mouvements de population, zones de conflit, etc.). Les enjeux de financement et d'équipement témoignent aussi d'une distribution inégale des ressources au sein de la communauté de défense des droits humains. Trevor A. Thrall *et al.* (2014) illustrent par exemple un cercle vicieux de concentration des ressources et de l'attention au sein du milieu des organisations non gouvernementales ; une poignée d'ONG décrites comme des *gatekeepers* dotées de budgets importants sont en mesure d'investir dans des ressources (scientifiques, sites web, vidéos) pour maximiser leur visibilité médiatique, laissant la grande majorité des autres organisations dans l'ombre.

Les limitations liées au renforcement des capacités renvoient au déficit de compétences et de moyens organisationnels pour maîtriser pleinement le cycle de vie de la donnée. La littérature identifie de faibles niveaux de littératie numérique (Strand et Svensson, 2023 ; Zanzoun, 2017) et d'expertise liée aux données et à leur visualisation (Rall *et al.*, 2016), voire des dissensions épistémiques au sein même des organisations sur l'impératif d'adopter des méthodes centrées sur les données (Freeman, 2021 ; Markland, 2021). Par ailleurs, la surabondance de données pouvant être analysées dans le cadre des enquêtes sur des violations menées par les défenseur·es des droits humains transforme un potentiel atout - l'abondance et la disponibilité de l'information - en un fardeau opérationnel, car les organisations ne disposent pas des ressources, ni des dispositions en termes de savoir-faire pour traiter et valoriser de grands volumes de données (Naimer *et al.*, 2017 ; Teo, 2025).

Les limitations liées à la sécurité numérique désignent, quant à elles, l'exposition constante et disproportionnée des défenseur·es des droits humains à des menaces qui exigent d'adopter des précautions qui sont décrites comme un fardeau (Michaelsen, 2018) qui s'étend à l'ensemble des réseaux activistes et à leurs familles. Le risque de voir la menace numérique se traduire en menace physique est jugé élevé en raison des capacités de collecte de données par les autorités et de violation de la vie privée, notamment du fait de failles

de sécurité dans les applications utilisées (Kazansky, 2015 ; Khamdamova, 2020 ; Naimer *et al.*, 2017). En outre, la gouvernance des données est caractérisée par un oligopole numérique transnational où les États et les Gafam exercent une emprise croissante sur les processus de mise en données. Cette centralisation crée une dépendance infrastructurelle critique qui exerce une contrainte sur l'autonomie des défenseur·es des droits humains dans leurs activités. La littérature mentionne à cet égard les règles arbitraires imposées par les plateformes et leur architecture centralisée qui offre des points d'accès privilégiés pour la surveillance, en exploitant par exemple les failles de sécurité ou les mesures insuffisantes de protection de l'anonymat (Gregory, 2019 ; Kazansky, 2015).

Les limitations liées aux médias réfèrent principalement à la manière dont la structure même de la sphère publique numérique est gouvernée par des acteurs privés qui manifestent une certaine passivité à garantir un environnement exempt de violence et de discrimination à l'égard des femmes militantes (Anstis et LaFlèche, 2025 ; Faith, 2022 ; Tripathi, 2022). Les médias socio-numériques sont aussi saturés sur le plan des contenus disponibles, limitant ainsi la portée et l'impact des récits portés par les défenseur·es des droits humains, mais aussi leur capacité à retrouver, à conserver puis à analyser des preuves visuelles publiées par des témoins. En effet, le fait de produire des données, même vérifiées, ne suffit pas à garantir leur impact : la modération (Fife *et al.*, 2023), désormais déléguée à des systèmes d'intelligence artificielle (Makhortykh, 2023) ainsi que la gouvernance algorithmique des plateformes, centrée sur l'optimisation de l'engagement des utilisateurs, contribuent à marginaliser les contenus militants (Della Valle et Simoncini, 2024 ; Gregory, 2019). Ce rapport de dépendance à l'égard des plateformes signifie que les contenus produits sont mis en concurrence avec des campagnes de désinformation et de *trolling* qui saturent l'espace médiatique et fragmentent l'opinion (Freeman, 2021 ; Kasm, 2018). À cet égard, Sam Gregory écrit : « *Actors hostile to human rights, from states to individuals, use the same technologies and platforms as human rights activists and community and grassroots journalists in order to spread misinformation, disinformation, and malinformation, to undermine civil society and democracy, and to perpetuate hate speech.* »⁸ (Gregory, 2019, p. 3-4).

Les limitations liées à l'environnement politique et aux cadres de régulation illustrent la manière dont le droit est souvent instrumentalisé pour entraver les activités des défenseur·es des droits humains et pour prévenir toute forme de contestation politique. Ces limitations concernent aussi les insuffisances du point de vue des normes d'utilisation des sources ouvertes (Murray *et al.*, 2022) et la rétention ou la falsification de preuves par les autorités (Rall *et al.*, 2016). Outre les règles d'utilisation contraignantes des plateformes et l'opacité de leur fonctionnement (Kazansky, 2015; Gregory, 2019; Faith, 2022), la littérature cite abondamment les lois sur la cybersécurité ou sur l'antiterrorisme qui sont fréquemment utilisées pour exiger la collaboration des entreprises privées, pour criminaliser les actes de collecte, de traitement et de diffusion de données par les défenseur·es des droits humains et, plus généralement, pour restreindre les possibilités d'action collective par le biais des technologies numériques (Della Valle et Simoncini, 2024 ; Illori, 2024 ; Nyst, 2018 ; Yingi et Benyera, 2024). La lente adoption de standards permettant l'intégration de preuves numériques devant les tribunaux internationaux dévalorise institutionnellement les fondements des activités d'enquête des défenseur·es des droits humains sur des données probantes.

Les limitations présentées précédemment ne constituent pas de simples obstacles : elles font état de vulnérabilités qui, suivant la critique des plateformes dont le modèle économique est fondé sur la monétisation de l'engagement (Kaun et Tréré, 2020), altèrent, d'une part, les capacités de mobilisation et amplifient, d'autre part, les discours haineux et la toxicité des échanges (Espindola, 2025). Le manque de capacité et de sécurité expose directement les défenseur·es des droits humains à la surveillance et au piratage, tandis que leur dépendance aux plateformes et la faiblesse des cadres juridiques contribuent davantage à leur marginalisation au sein d'un régime de gouvernance qui n'établit pas les normes de

protection et d'inclusion requises pour protéger leurs intérêts et pour reconnaître la précarité de leur situation.

Cet environnement de contraintes sociotechniques, bien que particulièrement hostile à l'action militante, agit aussi comme un catalyseur pour l'émergence de pratiques d'adaptation et d'innovation qui visent à créer des espaces d'autonomie et de sécurité. En mutualisant leurs infrastructures ou en contournant les normes officielles, les défenseur·es des droits humains ne sont pas seulement dans une posture défensive, ils expérimentent de nouvelles formes de gouvernance des données.

DES TACTIQUES DE RÉSISTANCE FACE À LA MISE EN ARMEMENT DES DONNÉES NUMÉRIQUES

La littérature scientifique met en lumière l'affirmation d'un phénomène d'« autoritarisme numérique » (Dragu et Lupu, 2021 ; Pearce et Kendzior, 2012) sur la scène internationale, positionnant *de facto* les données comme des instruments et des enjeux de pouvoir. Les adversaires des droits humains, en particulier les régimes autoritaires, exploitent les dispositifs numériques pour surveiller, pour censurer et pour intimider celles et ceux qui dénoncent leurs exactions. Les processus de mise en données participent ainsi à l'exercice et à la reproduction du pouvoir, et enjoignent les défenseur·es des droits humains à développer des stratégies défensives et de résistance au sein d'environnements numériques potentiellement hostiles où leurs pratiques les exposent à des risques accrus. Les analyses effectuées font émerger des pratiques illustrant des tactiques telles que la mutualisation des infrastructures (hébergement chiffré, *clouds* communautaires) et la formation continue pour renforcer les compétences en sécurité numérique, malgré des défis persistants soulignés par la littérature antérieure, notamment l'accès aux formations, la perception du risque et la disposition à s'engager volontairement pour développer ces compétences (Hankey et Ó Clunaigh, 2013 ; Kazansky, 2015 ; Kogan, 2013).

Sur le plan probatoire (certifier des preuves numériques et garantir la fiabilité des matériaux collectés), les défenseur·es des droits humains mettent en place des réseaux et des coalitions dans le but de mutualiser les ressources du point de vue technique, juridique et organisationnel (Acconcia *et al.*, 2024 ; Luna et Whetstone, 2024 ; Svensson *et al.*, 2024). Ils adoptent également une opacité tactique en utilisant par exemple des outils spécialisés comme *InformaCam* (van der Velden, 2015), pour sécuriser la collecte de données sensibles, mais aussi des tactiques fondées sur le *low-tech* (Hankey et Ó Clunaigh, 2013 ; MacLean, 2023) ou en fonction de la temporalité des conflits, comme l'écrivent Kirsty Fife *et al.* : « *Ownership and authorship of both records and archives need to be flexible in order to ensure security of creators and archivists, whilst also enabling the same people to later become more visible and named as central in the instrumentation of these projects* »⁹ (Fife *et al.*, 2023, p. 489). Enfin, les défenseur·es des droits humains contournent fréquemment les normes officielles en développant des méthodes d'archivage sécurisées. Des initiatives comme le *Syrian Archive*, *Mnemonic* ou le *858 Archive* mettent en œuvre cette pratique en archivant de vastes corpus documentaires de façon structurée. L'intégration de métadonnées et de protocoles de vérification à ce processus vise un triple objectif : prévenir la perte d'informations, garantir leur accessibilité et renforcer leur force probante dans le cadre de mécanismes de justice transitionnelle (Deutch et Al Khatib, 2018 ; Fife *et al.*, 2023 ; Kayyali, 2022).

Des propositions visant la création d'infrastructures d'accueil sécurisées pour les données sensibles semblables à des « cyber host States » (Marelli, 2020) et l'inclusion des défenseur·es des droits humains dans des espaces de délibération technique et réglementaire (Cath, 2021) - notamment auprès des acteurs économiques dans la conception de leurs outils et services techniques (Maréchal, 2015) - émergent par ailleurs dans les résultats d'analyse. Les stratégies de contournement adoptées par les défenseur·es des

droits humains révèlent ainsi les défaillances et les lacunes de la gouvernance des données à l'échelle locale, nationale et internationale. Elles mettent en évidence des normes internationales insuffisantes et des cadres juridiques inadaptés, tout en illustrant l'incapacité – ou le manque de volonté – des pouvoirs publics à instaurer des régimes crédibles et efficaces garantissant la responsabilité des acteurs qui entretiennent des pratiques numériques autoritaires et antidémocratiques.

VERS UNE DIPLOMATIE DES DONNÉES PAR LE BAS

L'étude présentée ici met en évidence la consolidation, dans la littérature récente, du constat d'un régime de répression numérique aux ramifications transnationales, où la mise en données devient un levier d'assujettissement des résistances sociales et politiques. À travers des usages comme la surveillance, la censure, la désinformation ou la criminalisation des activités militantes, les techniques numériques deviennent des outils qui entravent l'action des défenseur·es des droits humains. Cette répression s'appuie sur des vulnérabilités sociotechniques (inégalités d'accès, dépendance aux plateformes, opacité réglementaire, insécurité numérique, illégitimité des récits) qui restreignent l'autonomie des défenseur·es des droits humains dans l'usage des données et les exposent à des risques accrus.

Dans cet environnement hostile, les défenseur·es des droits humains développent des pratiques de contournement, de sécurisation et d'innovation qui ne relèvent pas seulement de la survie tactique. Elles dessinent les contours d'un rapport alternatif aux données, et constituent, à ce titre, des contributions politiques à part entière. Ces pratiques invitent à penser la diplomatie des données non comme une prérogative étatique ou technocratique, mais comme un champ disputé où se négocient des normes, des infrastructures et des représentations.

Pour appuyer ce constat, on peut évoquer les ressorts sur lesquels repose concrètement cette diplomatie des données construite « par le bas ». L'analyse du corpus identifie quatre dimensions constitutives qui, prises ensemble, confèrent aux pratiques des défenseur·es des droits humains une portée qui dépasse le registre de la simple résistance tactique pour s'inscrire dans celui de la production normative.

La première est celle des acteurs impliqués. Les pratiques recensées mettent en évidence une diversité de figures qui ne se réduit pas aux organisations de défense des droits humains au sens classique. Aux côtés des ONG établies et de leurs réseaux, les publications documentent le rôle croissant de collectifs d'enquête mobilisant les sources ouvertes (Deutch et Al Khatib, 2018), de coalitions transnationales spécialisées dans la collecte « forensic » comme *Physicians for Human Rights* et son outil *MediCapt* (Naimer *et al.*, 2017), de réseaux diasporiques qui prolongent l'action militante depuis l'exil (Tenove, 2019 ; Michaelsen, 2018), ou encore de communautés en ligne particulièrement exposées qui développent des pratiques de visibilité stratégique (Acconcia *et al.*, 2024 ; Svensson *et al.*, 2024). Ces acteurs partagent une caractéristique commune : ils opèrent à la marge des espaces institutionnels de délibération, et c'est précisément depuis cette position périphérique qu'ils contribuent à redéfinir les normes relatives aux données.

La deuxième dimension concerne les instruments déployés. La diplomatie des données « par le bas » ne repose pas sur des mécanismes formels de négociation, mais sur un ensemble d'outils et de protocoles qui matérialisent des choix normatifs. Le recours aux méthodes d'investigation en sources ouvertes (OSINT) dans certaines enquêtes internationales (Murray *et al.*, 2022) implique des protocoles de vérification rigoureux des données générées et partagées par des citoyens, traduisant de nouvelles normes de recevabilité probatoire. Des outils comme *InformaCam*, conçu pour intégrer des métadonnées de géolocalisation et d'horodatage au moment de la captation (van der Velden, 2015), ou encore les infrastructures d'archivage distribué développées par Syrian Archive et Mnemonic (Fife *et al.*, 2023 ; Kayyali, 2022), incarnent cette capacité à produire des standards techniques là

où les cadres officiels font défaut. La littérature souligne également l'importance des pratiques qui requièrent moins d'usages techniques (communément appelées *low-tech*), qui témoignent d'une adaptation aux contraintes matérielles des contextes d'intervention (Hankey et Ó Clunaigh, 2013 ; MacLean, 2023).

La troisième dimension est celle des espaces. Les défenseur·es des droits humains tentent d'investir des arènes de délibération hors des forums diplomatiques classiques. Les recherches mentionnent par exemple la participation aux instances de standardisation technique, à l'image des actions documentées par Corinne Cath (2021) au sein de l'*Internet Engineering Task Force* (IETF), des revendications d'inclusion dans la gouvernance des plateformes (Maréchal, 2015), ou encore des propositions concernant la création d'infrastructures d'accueil sécurisées pour les données sensibles, conçues comme des formes d'« asile numérique » (Marelli, 2020). Ces espaces se situent à l'intersection de la technique, du juridique et du politique où se négocient de manière informelle les règles qui déterminent la circulation et la valeur des données.

Enfin, la quatrième dimension est celle de la légitimité. À la différence de la diplomatie étatique, dont l'autorité découle d'un mandat politique formel, la légitimité des défenseur·es des droits humains dans le champ de la gouvernance des données repose sur d'autres fondements normatifs. Tout d'abord, la transparence méthodologique. Les protocoles de collecte, de vérification et d'authentification mis en œuvre dans les enquêtes en sources ouvertes renforcent la traçabilité qui constitue en elle-même une proposition normative puisqu'elle démontre qu'il est possible d'établir la fiabilité des données collectées hors des cadres institutionnels (Murray *et al.*, 2022 ; van der Velden, 2015). Ensuite, la vérifiabilité des données elles-mêmes. Les pratiques d'archivage structuré, d'intégration de métadonnées et de documentation des chaînes de conservation sont conçues pour favoriser la réplique et la contre-vérification par des tiers, qu'il s'agisse de chercheurs, de journalistes ou de juridictions (Deutch et Al Khatib, 2018 ; Fife *et al.*, 2023). Enfin, l'ancrage dans l'expérience située. La proximité avec les contextes de violation confère aux défenseur·es des droits humains une autorité épistémique fondée sur le témoignage direct et sur la connaissance pratique des conditions de terrain. Il s'agit d'une position que la littérature sur la gestion des visibilité en contexte répressif contribue à documenter (Albu, 2023). Ainsi, ces principes fondent la prétention des défenseur·es des droits humains à participer légitimement à la reconfiguration des normes de gouvernance des données et distinguent leur action d'un activisme numérique strictement orienté vers la mobilisation des publics et le plaidoyer pour sensibiliser les décideurs.

Ces quatre dimensions offrent la possibilité de saisir la cohérence interne de ce que nous désignons par « diplomatie des données par le bas ». De toute évidence, il ne s'agit pas d'une diplomatie formalisée dans des traités ou des protocoles internationaux, mais d'une diplomatie pratique, construite par accumulation d'initiatives convergentes. La structuration de cette diplomatie émerge de la conjonction d'acteurs qui se situent aux marges des institutions, d'instruments techniques qui matérialisent des exigences normatives, des espaces de délibération alternatifs où se négocient les règles du jeu, et une légitimité fondée non sur le mandat, mais sur la méthode. C'est dans cette perspective que la typologie de Boyd *et al.* (2019) peut être revisitée.

1. Une *diplomatie pour les données* : une diplomatie en soutien à la circulation et à la protection des données sensibles

Les pratiques documentées montrent que les défenseur·es des droits humains sont confrontés à des obstacles juridiques, techniques et politiques dans la collecte, la conservation, la transmission et la valorisation des données probantes. Une diplomatie des données centrée sur les droits humains devrait reconnaître le statut spécifique des données militantes sensibles ; garantir l'existence d'infrastructures d'asile numérique (archives sécurisées, cyberspaces protégés) ; promouvoir des standards de recevabilité internationale des preuves numériques dans les mécanismes de justice.

2. Des données pour la diplomatie : une diplomatie fondée sur la coopération par les données

Les pratiques de mutualisation, d'archivage collaboratif ou de plaidoyer fondées sur les données sont autant de formes de coopération transnationale entre défenseur·es des droits humains, journalistes, organisations non gouvernementales et chercheurs. Les données ne sont pas seulement un objet diplomatique, elles représentent aussi un médium relationnel. Elles peuvent constituer un vecteur de solidarité entre organisations exposées aux mêmes risques et servent à co-construire des narrations crédibles, à partir de multiples sources et contextes, face à la fragmentation informationnelle.

3. Une diplomatie des données partagée : une reconnaissance des défenseur·es des droits humains comme diplomates des données

Enfin, les défenseur·es des droits humains ne se contentent pas d'exiger des droits sur les données : ils produisent des récits, des savoirs et des normes. En tant que tels, ils participent activement à la fabrique diplomatique des données en rendant visibles des contextes minorés ou censurés, en questionnant les cadres dominants de légitimité, de preuve et de visibilité, et en expérimentant des formes alternatives de gouvernance informationnelle, plus décentralisées, plus sûres et plus éthiques.

Cette « diplomatie des données par le bas » ne se déploie pas de manière uniforme selon les contextes géopolitiques et sociotechniques dans lesquels elle s'inscrit. Dans les pays du « Sud global », les enjeux de dépendance infrastructurelle et de « fracture numérique » constituent des contraintes évidentes. L'accès même aux outils de collecte, de chiffrement ou d'archivage est inégalement distribué, et la gouvernance des données y est fréquemment structurée par des asymétries héritées de dynamiques coloniales (Couldry et Mejias, 2023), *a fortiori* dans les termes même des enjeux débattus dans les instances de délibération. À cet égard, Stefania Milan et Emiliano Treré (2019) défendent un renversement épistémique pour désenclaver des vécus dont la singularité est déniée. Ils mettent ainsi en garde contre un « universalisme des données » qui projette sur l'ensemble des contextes des catégories d'analyse forgées dans le « Nord global » et tend à invisibiliser les expériences situées. Dans le « Nord global », à l'inverse, la dépendance aux plateformes commerciales et la surveillance algorithmique constituent les contraintes dominantes, et la diplomatie « par le bas » prend davantage la forme de revendications d'inclusion dans les instances de standardisation et de régulation. Notre corpus, bien qu'anglophone, couvre une diversité de zones géographiques, de l'Ouganda (Strand et Svensson, 2023) à la République démocratique du Congo (Naimer *et al.*, 2017), du Zimbabwe (Yingi et Benyera, 2024) à la Syrie (Deutch et Al Khatib, 2018) ou la Tunisie (Della Valle et Simoncini, 2024), ce qui donne la possibilité d'observer cette diversité de configurations sans prétendre à l'exhaustivité.

Ces trois dimensions appellent à une redéfinition de la diplomatie des données non plus centrée sur les États et les grandes plateformes, mais ouverte aux savoirs situés, aux pratiques critiques et aux revendications normatives des acteurs vulnérables. Loin d'être de simples objets de protection, les défenseur·es des droits humains apparaissent alors comme des agents diplomatiques légitimes, porteurs d'un autre rapport à la vérité, à la mémoire, à la justice et à la circulation des savoirs.

CONCLUSION

L'autoritarisme numérique fondé sur la mise en données et sa mise en armement reconfigure profondément les rapports de pouvoir et expose les défenseur·es des droits humains à des risques accrus. En rendant visibles les régimes de surveillance, de censure et de propagande, ainsi que les vulnérabilités matérielles, infrastructurelles et juridiques qui les soutiennent, notre revue met en évidence deux contributions.

Elle documente, d'une part, un répertoire robuste et convergent de tactiques militantes

telles que la mutualisation d'infrastructures, la sécurisation des preuves, l'archivage distribué, les coopérations via des réseaux transnationaux, qui dessinent les contours d'une « diplomatie des données par le bas ». Face à cette mise en armement des données, les stratégies de résistance développées par les défenseur·es des droits humains ne peuvent être réduites à de simples ajustements techniques ; elles constituent une contestation implicite des modèles de gouvernance dominants, articulée autour de trois principes opérationnels que sont la protection (sécurité, intégrité et dignité des personnes et des données), le partage et la traçabilité (interopérabilité, préservation et authenticité des chaînes de preuve) et la participation (inclusion des défenseur·es des droits humains dans les arènes de standardisation, de régulation et de modération).

L'analyse révèle, d'autre part, les insuffisances des cadres juridiques actuels et ouvre la voie à des orientations concrètes telles que la reconnaissance d'un statut protecteur des données militantes sensibles, la garantie de la recevabilité des preuves numériques par des standards de collecte et des obligations de conservation, le renforcement des devoirs de vigilance et de transparence des plateformes, l'encadrement de la répression numérique transnationale par la clarification des responsabilités extraterritoriales, et les garanties procédurales pour les défenseur·es des droits humains.

Ce cadre interprétatif prospectif rencontre toutefois deux limites qu'il convient de formuler explicitement. La première est d'ordre méthodologique. En effet, la « diplomatie des données par le bas » émerge ici d'une revue de la littérature savante, et ne saurait capturer toute la complexité du vécu des acteurs de terrain. La manière dont les individus et les collectifs militants perçoivent leurs propres actions, négocient les risques au quotidien et donnent sens à leur engagement numérique reste un impensé de notre démarche dont l'approfondissement parviendrait à mieux inscrire les enjeux discutés dans un agenda de recherche susceptible de dépasser les limites des conceptions dominantes de la régulation de la production et des usages des données (Milan et Tréré, 2019). La seconde limite est d'ordre juridique. La fragmentation des régimes existants relatifs à la circulation transnationale des données, à la protection des informations probantes et à la responsabilité des plateformes rend délicates voire erronées les tentatives d'articuler les pratiques recensées et les instruments juridiques disponibles, qu'ils soient contraignants ou souples.

Ces limites dessinent deux chantiers prioritaires : éprouver empiriquement le cadre proposé par des entretiens et des observations auprès des défenseur·es des droits humains, afin de saisir les stratégies telles qu'elles sont vécues en contexte, et croiser l'analyse des pratiques avec une cartographie fine des régulations existantes (preuve numérique, protection des sources, cybersécurité, devoir de vigilance, export de technologies intrusives), pour identifier les leviers d'évolution et mesurer l'écart entre le droit positif et les attentes révélées.

L'essor rapide de l'intelligence artificielle générative confère une urgence supplémentaire aux chantiers mentionnés. L'IA « mise en armement » amplifie simultanément les capacités de répression par la génération d'hypertrucages destinés à discréditer des défenseur·es des droits humains (Gregory, 2022), par l'automatisation de la modération qui marginalise les contenus militants et dissidents (Makhortykh, 2023), ou par la « violence lente » qu'elle est en mesure de contribuer à exercer sur les droits fondamentaux (Teo, 2025), et les capacités de contre-surveillance, en offrant des outils d'analyse automatisée de preuves visuelles et de détection de contenus falsifiés (Freeman, 2021). La gouvernance des systèmes d'IA et de leurs données d'entraînement constitue dès lors un terrain émergent de diplomatie des données où les voix des acteurs les plus vulnérables demeurent largement absentes.

NOTES

¹ Le concept d'autoritarisme numérique renvoie à l'usage, par des États, d'un ensemble articulé de mesures, de processus et de dispositifs numériques à des fins antidémocratiques (voir Glasius et Michaelsen, 2018). Il se manifeste notamment par le contrôle et la manipulation de l'information, la surveillance (ciblée ou généralisée) des populations, les intrusions dans les systèmes, la destruction de données et d'infrastructures, ainsi que la perturbation des activités des opposants. Ces pratiques font peser des menaces directes sur la sécurité des individus et contribuent à restreindre leur capacité d'action autonome.

² Les contraintes sociotechniques désignent les limitations à l'action qui émergent de l'articulation complexe entre les architectures techniques (infrastructures numériques, plateformes et dispositifs de traitement de données) et les structures sociales, façonnées par les rapports de pouvoir, les cadres réglementaires, les normes et les inégalités d'accès et d'usage aux ressources. Elles se construisent dans l'interaction dynamique entre pratiques, dispositifs et rapports de pouvoir, modulant de manière différenciée les capacités d'agir, les marges de manœuvre et les zones de vulnérabilité des acteurs (voir Coutant, 2015, sur les approches sociotechniques).

³ Les bases de données retenues sont les suivantes : *HeinOnline - Law Journal Library* ; *Brill Online Books : Human Rights and Humanitarian Law* ; *Oxford scholarship Online - Law* ; *Scopus (Elsevier)* ; *CANLII* ; *ProQuest* ; *Google Scholar*.

⁴ Les équations détaillées de la phase 2 sont les suivantes : (a) (« human rights defenders » OR « human rights activists ») AND (« digital technologies » OR « information and communication technologies » OR « social media » OR « digital platforms ») ; (b) idem AND (« digital security » OR « surveillance » OR « censorship » OR « repression » OR « online harassment ») ; (c) idem AND (« online mobilization » OR « digital activism » OR « social media » OR « freedom of expression ») ; (d) idem AND (« data protection » OR « technology legislation » OR « internet governance » OR « hate speech » OR « disinformation »).

⁵ Les revues concernées sont les suivantes : *International Journal on Human Rights*, *Human Rights Quarterly*, *The International Human Rights Law Review*, *Asia-Pacific Journal on Human Rights and the Law*, *Journal of Human Rights Practice*, et *International Review of the Red Cross*.

⁶ Le choix d'un corpus exclusivement anglophone est délibéré, fondé sur trois constats issus du processus de recension. Premièrement, les recherches exploratoires sur les bases francophones (Cairn, Érudit, Persée) ont révélé une rareté notable de publications spécifiques à l'articulation pratiques numériques / droits humains. Deuxièmement, la variabilité terminologique en français (« droits humains », « droits de l'homme », « droits de la personne ») complexifie considérablement la systématisation et introduit un risque d'incomplétude. Troisièmement, l'objectif de l'étude était précisément de cartographier la manière dont la littérature internationale, dont l'anglais est *de facto* la langue véhiculaire dans les revues à comité de lecture, traite de cette problématique.

⁷ Les écrits mentionnent le logiciel espion Pegasus développé par l'entreprise israélienne *NSO Group* comme outil fréquemment déployé pour mettre en place cette surveillance ; qualifié de technologie posant des « risques sans précédent » par le Contrôleur européen de la protection des données (Anstis, 2024), le logiciel accorde à son opérateur un accès total au téléphone ciblé, y compris le contenu d'applications chiffrées comme *Signal* ou *WhatsApp*, ainsi qu'au micro et à la caméra du dispositif numérique.

⁸ « Les acteurs hostiles aux droits humains, qu'il s'agisse d'États ou d'individus, utilisent les mêmes techniques et plateformes que les militant·es des droits humains et les journalistes communautaires et de terrain afin de propager la mésinformation, la désinformation et les informations malveillantes, de saper la société civile et la démocratie, et de perpétuer les discours de haine. » (Gregory, 2019, p. 3-4, notre traduction).

⁹ « La propriété et la paternité des documents comme des archives doivent être suffisamment flexibles pour, d'une part, garantir la sécurité des créateurs et des archivistes, et d'autre part, permettre à ces mêmes personnes d'être ultérieurement reconnues et de gagner en visibilité en tant que figures centrales dans la conduite de ces projets. » (Fife *et al.*, 2023, p 489, notre traduction).

RÉFÉRENCES BIBLIOGRAPHIQUES

Acconcia, Giovanni ; Perego, Alessandro ; Perini, Luca (2024), « LGBTQ activism in repressive contexts: The struggle for (in)visibility in Egypt, Tunisia and Turkey », *Social Movement Studies*, vol. 23, n° 2, p. 207-225.

Albu, Oana B. (2023), « Managing visibilities: The shades and shadows of NGO work in repressive contexts », *Management Communication Quarterly*, vol. 37, n° 3, p. 659-685.

Anstis, Siena (2024), « Regulating transnational dissident cyber espionage », *International & Comparative Law Quarterly*, vol. 73, n° 1, p. 259-274.

Anstis, Siena ; Barnett, Sarah (2022), « Digital transnational repression and host states' obligation to protect against human rights abuses », *Journal of Human Rights Practice*, vol. 14, n° 2, p. 698-725.

Anstis, Siena ; LaFlèche, Émilie (2025), « Gender-based digital transnational repression as a global authoritarian practice », *Globalizations*, vol. 22, n° 4, p. 671-688.

Assemblée générale des Nations Unies (1999), *Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnues (A/RES/53/144)*, New York : Organisation des Nations Unies.

Belmonte, Laura (2023), « Can human rights survive technology? », *Diplomatic History*, vol. 47, n° 1, p. 1-18.

Benford, Robert D. ; Snow, David A. ; Plouchard, Nicolas M. (2012), « Processus de cadrage et mouvements sociaux : présentation et bilan », *Politix*, n° 99, p. 217-255.

Boyd, Andrew ; Gatewood, Justin ; Thorson, Stuart ; Dye, Thomas D. V. (2019), « Data diplomacy », *Science & Diplomacy*, vol. 8, n° 1, [en ligne], consulté le 24 septembre 2025, <http://sciencediplomacy.org/article/2019/data-diplomacy>.

Bradshaw, Samantha ; Howard, Philip N. (2019), *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, Oxford : Oxford Internet Institute (Computational Propaganda Project).

Brough, Melissa ; Li, Zhen (2013), « Media systems dependency and human rights online video: The "Saffron Revolution" and WITNESS's Hub », *International Journal of Communication*, vol. 7, p. 281-304.

Bullich, Vincent ; Clavier, Viviane (2019), « Production des données, 'Production de la société'. Les Big Data et algorithmes au regard des Sciences de l'information et de la communication », *Les Enjeux de l'information et de la communication*, vol. 19, n° 2, p. 5-14.

Cascio, M. Ariel ; Lee, Eunlye ; Vaudrin, Nicole ; Freedman, Darcy A. (2019), « A team-based approach to open coding: Considerations for creating intercoder consensus », *Field Methods*, vol. 31, n° 2, p. 116-130.

Cath, Corinne (2021), « The technology we choose to create: Human rights advocacy in the Internet Engineering Task Force », *Telecommunications Policy*, vol. 45, n° 6, [en ligne], consulté le 30 avril 2026, <https://doi.org/10.1016/j.telpol.2021.102144>.

Chubb, Andrew ; Roberts Lyer, Kira (2024), « Transnational human rights violations: Addressing the evolution of globalized repression through national human rights institutions », *Journal of Human Rights Practice*, vol. 16, n° 3, p. 770-793.

Costanza-Chock, Sasha (2020), *Design Justice: Community-Led Practices to Build the Worlds We Need*, Cambridge : The MIT Press.

Couldry, Nick ; Mejias, Ulises A. (2023), « The decolonial turn in data and technology research: What is at stake and where is it heading? », *Information, Communication & Society*, vol. 26, n° 4, p. 786-802.

Coutant, Alexandre (2015), « Les approches sociotechniques dans la sociologie des usages en SIC », *Revue française des sciences de l'information et de la communication*, n° 6, [en ligne], consulté le 30 avril 2026, <https://doi.org/10.4000/rfsic.1271>.

Deibert, Ronald (2015), « Authoritarianism goes global: Cyberspace under siege », *Journal of Democracy*, vol. 26, n° 3, p. 64-78.

Della Valle, Chiara ; Simoncini, Giulia (2024), « Shades of presence in post-2011 Tunisia: Evolving political positions in feminist and queer activism », *Contemporary Politics*, p. 1-22.

Denouël, Julie ; Granjon, Fabien (2011), (dir.), *Communiquer à l'ère numérique. Regards croisés sur la sociologie des usages*, Paris : Presses des Mines.

Deutch, Jessica ; Al Khatib, Hadi (2018), « The Syrian Archive: A methodological case study of open-source investigation of state crime using video evidence from social media platforms », *State Crime Journal*, vol. 7, n° 1, [en ligne], consulté le 30 avril 2026, <https://doi.org/10.13169/statecrime.7.1.0046>.

Diamond, Larry (2010), « Liberation technology », *Journal of Democracy*, vol. 21, n° 3, p. 69-83.

Dragu, Tiberiu ; Lupu, Yonatan (2021), « Digital authoritarianism and the future of human rights », *International Organization*, vol. 75, n° 4, p. 991-1017.

Eguridu, Hope ; Tolani, Tolu ; Olusola, Opeyemi ; Sakpere, Wilson (2024), « Impact of information technology on civil rights and criminal liabilities », *African Journal of Law, Ethics and Education*, vol. 7, n° 1, [en ligne], consulté le 30 avril 2026, <https://ajleejournal.com/index.php/ajlee/article/view/168>.

El Gody, Ahmed (2022), « The revolution continues: Mapping the Egyptian Twittersphere a decade after the 2011 Revolution », *First Monday*, vol. 27, n° 8, [en ligne], consulté le 30 avril 2026, <https://doi.org/10.5210/fm.v27i8.11775>.

Espíndola, José (2025), « Attributing responsibility to Big Tech for mass atrocity: Social media and transitional justice », *Perspectives on Politics*, vol. 23, n° 3, p. 1-15.

Faith, Becky (2022), « Tackling online gender-based violence; understanding gender, development, and the power relations of digital spaces », *Gender, Technology and Development*, vol. 26, n° 3, p. 325-340.

Fife, Kirsty ; Flinn, Andrew ; Nyhan, Julianne (2023), « Documenting resistance, conflict and violence: A scoping review of the role of participatory digital platforms in the mobilisation of resistance », *Archival Science*, vol. 23, n° 3, p. 471-499.

Freeman, Lindsay (2021), « Weapons of war, tools of justice: Using artificial intelligence to investigate international crimes », *Journal of International Criminal Justice*, vol. 19, n° 1, p. 35-53.

Glasius, Marlies ; Michaelsen, Marcus (2018), « Illiberal and authoritarian practices in the digital sphere. Prologue », *International Journal of Communication*, vol. 12, p. 3795-3813.

Gregory, Sam (2010), « Cameras everywhere: Ubiquitous video documentation of human

rights, new forms of video advocacy, and considerations of safety, security, dignity and consent », *Journal of Human Rights Practice*, vol. 2, n° 2, p. 191-207.

Gregory, Sam (2019), « Cameras everywhere revisited: How digital technologies and social media aid and inhibit human rights documentation and advocacy », *Journal of Human Rights Practice*, vol. 11, n° 2, p. 373-392.

Gregory, Sam (2022), « Deepfakes, misinformation and disinformation and authenticity infrastructure responses: Impacts on frontline witnessing, distant witnessing, and civic journalism », *Journalism*, vol. 23, n° 3, p. 708-729.

Gregory, Sam (2023), « Fortify the truth: How to defend human rights in an age of deepfakes and generative AI », *Journal of Human Rights Practice*, vol. 15, n° 3, p. 702-714.

Hankey, Stephanie ; Ó Clunaigh, Daniel (2013), « Rethinking risk and security of human rights defenders in the digital age », *Journal of Human Rights Practice*, vol. 5, n° 3, p. 535-547.

Herscher, Andrew (2014), « Surveillant witnessing: Satellite imagery and the visual politics of human rights », *Public Culture*, vol. 26, n° 3, p. 469-500.

Ilori, Tunde (2024), « Protecting digital rights through soft law: Ensuring the implementation of the revised Declaration of Principles on Freedom of Expression and Access to Information in Africa », *African Human Rights Law Journal*, vol. 24, n° 1, p. 1-30.

Kane, Oumar (2013), « Les usages des TIC entre analyse sociotechnique et théories de l'appropriation : état de la littérature », *Les Enjeux de l'information et de la communication*, p. 23-42, [en ligne], consulté le 18 novembre 2025, <https://www.academia.edu/7277534>.

Kasm, Shady (2018), « Redefining publics: Mosireen, state crime and the rise of a digital public sphere », *State Crime Journal*, vol. 7, n° 1, [en ligne], consulté le 30 avril 2026, <https://doi.org/10.13169/statecrime.7.1.0100>.

Kaun, Anne ; Treré, Emiliano (2020), « Repression, resistance and lifestyle: Charting (dis)connection and activism in times of accelerated capitalism », *Social Movement Studies*, vol. 19, n° 5-6, p. 697-715.

Kayyali, Dia (2022), « Digital memory, evidence, and social media. Lessons learned from Syria », *Sociologica*, vol. 16, n° 2, p. 253-259.

Kazansky, Becky (2015), « FCJ-195 Privacy, responsibility, and human rights activism », *The Fibreculture Journal*, n° 26, p. 190-208.

Khamdamova, Feruza (2020), « The impact of digital technologies on human rights », *TSUL Legal Report International electronic scientific journal*, vol. 1, n° 1, [en ligne], consulté le 30 avril 2026, <https://legalreport.tsul.uz/index.php/journal/article/view/21>.

Kogan, Vladimir (2013), « Protecting human rights defenders in the North Caucasus: Reflections on developments from 2009 to the present », *Journal of Human Rights Practice*, vol. 5, n° 3, p. 500-511.

Land, Molly K. ; Aronson, Jay D. (2020), « Human rights and technology: New challenges for justice and accountability », *Annual Review of Law and Social Science*, vol. 16, n° 1, p. 223-240.

Landry, Normand ; Aubin, France ; Sénécal, Michel (2015), « Médias et mouvements sociaux: pratiques de mobilisations collectives », *Canadian Journal of Media Studies / Revue canadienne d'études médiatiques*, vol. 13, n° 1, p. 124-144, [en ligne], consulté le 30 avril 2026, <http://cjms.fims.uwo.ca/issues/13-01/Landry.pdf>.

Landry, Normand ; Hocine, Julien ; Fitzbay, Simon ; Dupuis, Marie-Josée (2025), « Pratiques numériques et mise en données de la défense des droits humains », *Communication*, vol. 42, n° 2, [en ligne], consulté le 30 avril 2026, <https://doi.org/10.4000/15bo5>.

Lievrouw, Leah A. (2023), *Alternative and Activist New Media*, 2e éd., Cambridge : Polity Press.

Locke, Karen ; Feldman, Martha ; Golden-Biddle, Karen (2022), « Coding practices and iterativity: Beyond templates for analyzing qualitative data », *Organizational Research Methods*, vol. 25, n° 2, p. 262-284.

Luna, Krishna C. ; Whetstone, Crystal (2024), « Women, peace and security: Digitalization and cyber feminist solidarity building in the global South », *Women's Studies International Forum*, vol. 105, [en ligne], consulté le 30 avril 2026, <https://www.sciencedirect.com/science/article/pii/S0277539524000906>.

Lyon, David (2015), *Surveillance after Snowden*, Cambridge : Polity Press.

Lyubareva, Inna ; Nocetti, Julien ; Carey-Libbrecht, Loïc (2024), « Digital diplomacy: Evolution of diplomatic and influence strategies in the digital age », *Réseaux*, n° 245, p. 11-35.

MacLean, Kate (2023), « Interactive digital platforms, human rights fact production, and the International Criminal Court », *Journal of Human Rights Practice*, vol. 15, n° 1, p. 84-99.

Makhortykh, Mykola (2023), « Unreliable narrators or untimely archivists? Challenges of using digital platforms for documenting and remembering Russia's war in Ukraine », *Georgetown Journal of International Affairs*, vol. 24, n° 2, p. 165-173.

Maréchal, Nathalie (2015), « Ranking Digital Rights: Keeping the internet safe for advocacy », *The Fibreculture Journal*, n° 26, p. 302-308.

Marelli, Massimo (2020), « Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation », *International Review of the Red Cross*, vol. 102, n° 913, p. 367-387.

Markland, Adam (2021), « Epistemic transformation at the margins: Resistance to digitalisation and datafication within global human rights advocacy », *Global Society*, vol. 36, n° 1, p. 113-133.

McNutt, John G. (2018), (dir.), *Technology, Activism, and Social Justice in a Digital Age*, New York : Oxford University Press.

Meikle, Graham (2018), (dir.), *The Routledge Companion to Media and Activism*, London : Routledge.

Michaelsen, Marcus (2018), « Exit and voice in a digital age: Iran's exiled activists and the authoritarian state », *Globalizations*, vol. 15, n° 2, p. 248-264.

Michaelsen, Marcus ; Glasius, Marlies (2018), « Authoritarian practices in the digital age — Introduction », *International Journal of Communication*, vol. 12, p. 7.

Milan, Stefania (2013), *Social Movements and Their Technologies: Wiring Social Change*, Basingstoke : Palgrave Macmillan.

Milan, Stefania ; Treré, Emiliano (2019), « Big data from the South(s): Beyond data universalism », *Television & New Media*, vol. 20, n° 4, p. 319-335.

Morozov, Evgeny (2011), *The Net Delusion: The Dark Side of Internet Freedom*, 1re éd., New York : Public Affairs.

Mosco, Vincent (2016), « Après l'Internet : le Cloud, les big data et l'Internet des objets », *Les Enjeux de l'information et de la communication*, vol. 17, n° 2, p. 145-155.

Murray, David ; Fussey, Pete ; Hove, Kennedy ; Wakabi, Wairagala ; Kimumwe, Peter ; Saki, Obert ; Stevens, Alex (2024), « The chilling effects of surveillance and human rights: Insights from qualitative research in Uganda and Zimbabwe », *Journal of Human Rights Practice*, vol. 16, n° 1, p. 397-412.

Murray, David ; McDermott, Yvonne ; Koenig, Kristen A. (2022), « Mapping the use of open source research in UN human rights investigations », *Journal of Human Rights Practice*, vol. 14, n° 2, p. 554-581.

Nah, Alice M. ; Bennett, Karen ; Ingleton, Debbie ; Savage, James (2013), « A research agenda for the protection of human rights defenders », *Journal of Human Rights Practice*, vol. 5, n° 3, p. 401-420.

Naimer, Karen ; Brown, William ; Mishori, Ranit (2017), « MediCapt in the Democratic Republic of the Congo: The design, development, and deployment of mobile technology to document forensic evidence of sexual violence », *Genocide Studies and Prevention*, vol. 11, n° 1, p. 25-35.

Nissen, Anne (2023), « Gender-transformative remedies for women human rights defenders », *Business and Human Rights Journal*, vol. 8, n° 3, p. 369-402.

Nwagwu, Williams E. (2025), « Datafication research (1994-2023) : Three decades of evolving methodology in data science », *Topoi*, vol. 44, p. 1049-1070.

Nyst, Carly (2018), « Secrets and lies: The proliferation of state surveillance capabilities and the legislative secrecy which fortifies them — An activist's account », *State Crime Journal*, vol. 7, n° 1, p. 8-23.

Oral, Ece (2024), « The environmental rule of law and the protection of human rights defenders: Law, society, technology, and markets », *International Environmental Agreements: Politics, Law and Economics*, vol. 24, n° 2-3, p. 393-421.

Pearce, Katy E. ; Kendzior, Sarah (2012), « Networked authoritarianism and social media in Azerbaijan », *Journal of Communication*, vol. 62, n° 2, p. 283-298.

Rall, Kirsten ; Satterthwaite, Margaret L. ; Pandey, Abhishek V. ; Emerson, John ; Boy, Jeremy ; Nov, Oded ; Bertini, Enrico (2016), « Data visualization for human rights advocacy », *Journal of Human Rights Practice*, vol. 8, n° 2, p. 171-197.

Shahbaz, Adrian (2018), « Fake news, data collection, and the challenge to democracy. Freedom on the Net 2018: The rise of digital authoritarianism », *Freedom House*, [en ligne], consulté le 29 septembre 2025, <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism>.

Siatitsa, Ilia (2020), « Freedom of assembly under attack: General and indiscriminate surveillance and interference with internet communications », *International Review of the Red Cross*, vol. 102, n° 913, p. 181-198.

Stevens, Alex ; Fussey, Pete ; Murray, David ; Hove, Kennedy ; Sake, Obert (2023), « "I started seeing shadows everywhere": The diverse chilling effects of surveillance in Zimbabwe », *Big Data & Society*, vol. 10, n° 1, p. 1-14.

Strand, Cecilia ; Svensson, Jakob (2023), « Towards a situated understanding of vulnerability — An analysis of Ugandan LGBT+ exposure to hate crimes in digital spaces », *Journal of Homosexuality*, vol. 70, n° 12, p. 2806-2827.

Svensson, Jakob ; Larsson, Anders O. ; Strand, Cecilia (2024), « Who relates to whom and according to which rationale? Visibility and advocacy in the Ugandan LGBT+ Twittersphere », *New Media & Society*, vol. 27, n° 7, [en ligne], consulté le 30 avril 2026, <https://doi.org/10.1177/14614448241236853>.

Tenove, Chris (2019), « Networking justice: digitally-enabled engagement in transitional justice by the Syrian diaspora », *Ethnic and Racial Studies*, vol. 42, n° 11, p. 1950-1969.

Teo, Sherly A. (2025), « Artificial intelligence and its "slow violence" to human rights », *AI and Ethics*, vol. 5, p. 2265-2280.

Thrall, A. Trevor ; Stecula, Dominik ; Sweet, Diana (2014), « May we have your attention

please? Human-rights NGOs and the problem of global communication », *The International Journal of Press/Politics*, vol. 19, n° 2, p. 135-159.

Tilly, Charles (1995), *Popular Contention in Great Britain, 1758-1834*, Cambridge : Harvard University Press.

Tilly, Charles ; Tarrow, Sidney (2015), *Contentious Politics*, 2e éd., New York : Oxford University Press.

Torraco, Richard J. (2016), « Writing integrative literature reviews: Guidelines and examples », *Human Resource Development Review*, vol. 15, n° 4, [en ligne], consulté le 30 avril 2026, <https://doi.org/10.1177/1534484316671606>.

Tripathi, Srishti (2022), « Women and online harassment », *Feminist Dissent*, n° 6, p. 133-158.

Tufekci, Zeynep (2017), *Twitter and Tear Gas: The Power and Fragility of Networked Protest*, New Haven : Yale University Press.

van der Velden, Lonneke (2015), « Forensic devices for activism: Metadata tracking and public proof », *Big Data & Society*, vol. 2, n° 2, [en ligne], consulté le 30 avril 2026, <https://doi.org/10.1177/2053951715612823>.

Wilson, Richard A. (2022), « Digital authoritarianism and the global assault on human rights », *Human Rights Quarterly*, vol. 44, n° 4, p. 704-739.

Yingi, Emmanuel ; Benyera, Everisto (2024), « The future of democracy in the digital era: Internet shutdowns, cyber laws and online surveillance in Zimbabwe », *Alternatives: Global, Local, Political*, vol. 50, n° 2, [en ligne], consulté le 30 avril 2026, <https://doi.org/10.1177/03043754241259878>.

Zanzoun, Mustapha (2017), « The use of social media in promoting human rights among speakers of English in Morocco: The case of Facebook », *International Journal of Education and Research*, vol. 5, n° 9, p. 169-184.

Zuboff, Shoshana (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York : Public Affairs.