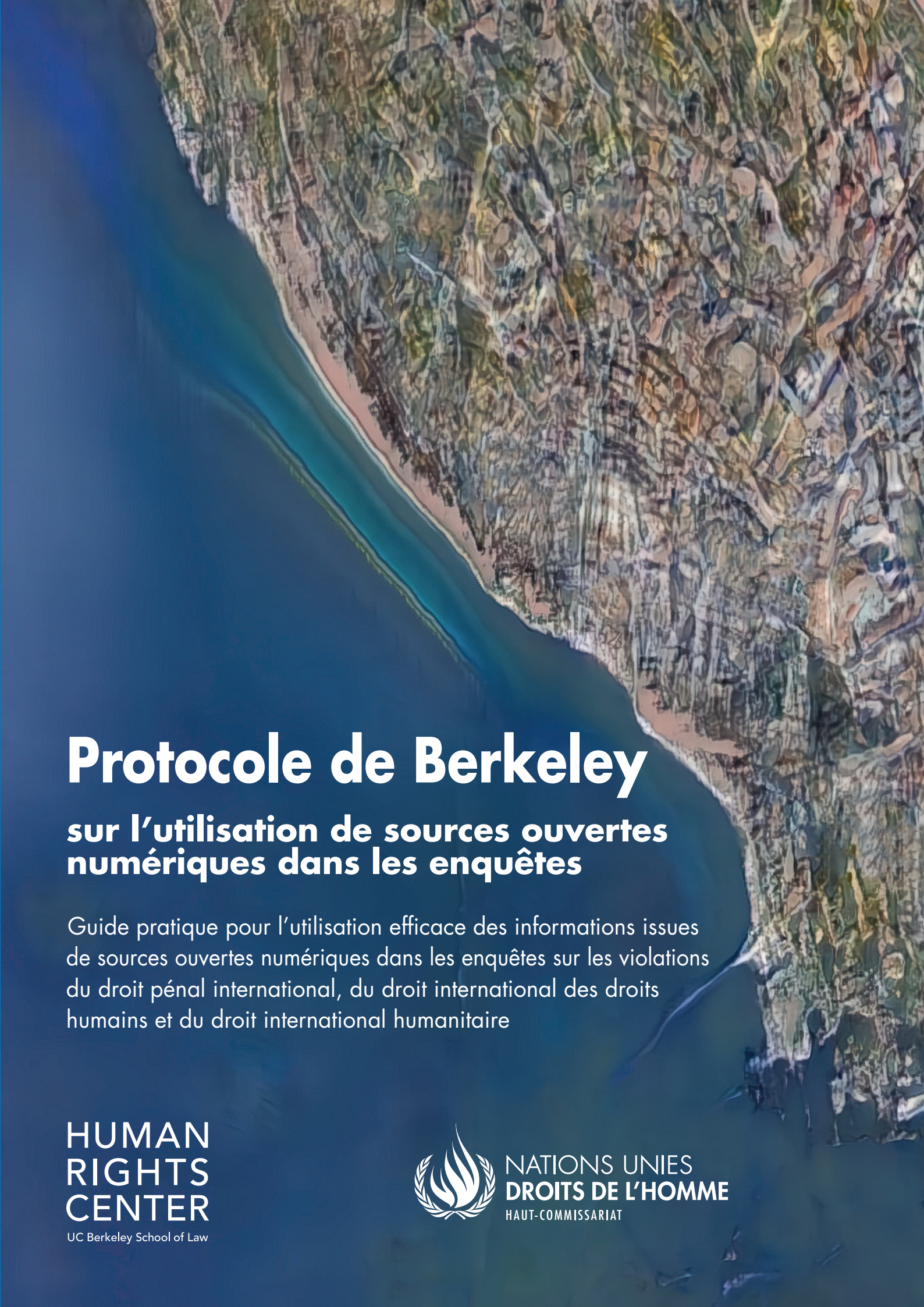


Protocole de Berkeley

sur l'utilisation de sources ouvertes numériques dans les enquêtes

Guide pratique pour l'utilisation efficace des informations issues de sources ouvertes numériques dans les enquêtes sur les violations du droit pénal international, du droit international des droits humains et du droit international humanitaire

HUMAN RIGHTS CENTER
UC Berkeley School of Law

NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

Protocole de Berkeley

sur l'utilisation de sources ouvertes numériques dans les enquêtes

Guide pratique pour l'utilisation efficace des informations issues de sources ouvertes numériques dans les enquêtes sur les violations du droit pénal international, du droit international des droits humains et du droit international humanitaire

HUMAN RIGHTS CENTER
UC Berkeley School of Law

NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

New York et Genève, 2024

HR/PUB/20/2
ISBN : 978-92-1-154245-5
eISBN : 978-92-1-005344-0
Numéro de vente : F.20.XIV.4

Le présent ouvrage est copublié par les Nations Unies, pour le compte du Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH), et le Human Rights Center de la faculté de droit de l'Université de Californie à Berkeley.

Les appellations employées dans la présente publication et la présentation des données qui y figurent n'impliquent, de la part du Secrétariat de l'Organisation des Nations Unies, aucune prise de position quant au statut juridique des pays, territoires, villes ou zones, ou de leurs autorités, ni quant au tracé de leurs frontières ou limites.

Les cotes des documents de l'Organisation des Nations Unies se composent de lettres majuscules et de chiffres. La simple mention d'une cote dans un texte signifie qu'il s'agit d'un document de l'Organisation.

Crédit image de la page de couverture : image satellitaire hypertruquée créée par Ahmed Elgamal au moyen de la plateforme d'intelligence artificielle Playform.

Le Human Rights Center de la faculté de droit de l'Université de Californie à Berkeley remercie de leur soutien financier les donateurs suivants : le Sigrid Rausing Trust, la Oak Foundation, des particuliers à l'Université de Californie à Berkeley, les Open Society Foundations et le Bellagio Center de la Fondation Rockefeller.

TABLE DES MATIÈRES

Avant-propos v

Résumé introductif ix

Collaborations et participations x

Abréviations xiv

I. INTRODUCTION 1

A. Objet 4

B. Public 5

C. Définitions 6

II. PRINCIPES 11

A. Principes professionnels 13

B. Principes méthodologiques 15

C. Principes déontologiques 17

III. CADRE JURIDIQUE 19

A. Droit international public 22

B. Compétence et responsabilité 25

C. Pouvoirs et devoirs d'enquête 26

D. Règlements de procédure et de preuve ... 28

E. Droit à la vie privée et protection des données 30

F. Autres considérations juridiques pertinentes 31

IV. SÉCURITÉ 33

A. Normes minimales 35

B. Évaluations de la sécurité 36

C. Considérations relatives à l'infrastructure 41

D. Considérations relatives aux utilisateurs 44

V. PRÉPARATION 47

A. Évaluation des menaces et des risques .. 49

B. Appréciation du paysage numérique 49

C. Plan d'enquête en ligne 51

D. Plan de résilience et autosoins 52

E. Politiques et outils relatifs aux données .. 54

VI. TÂCHES DE L'ENQUÊTE 57

A. Investigations en ligne 60

B. Appréciation préliminaire 62

C. Collecte 63

D. Conservation 64

E. Vérification 67

F. Analyse d'enquête 71

VII. RAPPORT D'ENQUÊTE 75

A. Rapport écrit 77

B. Rapport oral 78

C. Rapport visuel 79

VIII. GLOSSAIRE 81

ANNEXES 87

I. Modèle de plan d'enquête en ligne 89

II. Modèle d'évaluation des menaces et des risques numériques 90

III. Modèle d'état des lieux du paysage numérique 91

IV. Formulaire de collecte de données en ligne 92

V. Considérations pour la validation de nouveaux outils 93

Avant-propos

Depuis le début des années 1990, les outils numériques et Internet, tout comme l'appareil photographique et le téléphone avant eux, ont révolutionné la façon dont nous cherchons, recueillons et diffusons l'information relative aux violations des droits humains et à d'autres violations graves du droit international, dont les crimes internationaux.

Aujourd'hui, les enquêteurs peuvent extraire des données relatives à ces violations et ces crimes éventuels d'un vaste éventail d'images satellites, de vidéos et de photos accessibles au public, notamment d'informations téléversées sur Internet au moyen de smartphones ou publiées sur les plateformes de réseaux sociaux. Cette possibilité a permis aux enquêteurs de contourner les gouvernements et autres contrôleurs de l'information pour obtenir, en temps réel même, des informations cruciales sur des agissements qui, autrement, seraient restés cachés du public.

Les informations de sources ouvertes numériques n'ont cependant été utilisées que d'une manière souvent ponctuelle, les organismes de défense des droits humains, les organes intergouvernementaux, les mécanismes d'enquête et les tribunaux ayant parfois peiné à intégrer de nouvelles techniques numériques d'établissement des faits et d'analyse dans leurs méthodes de travail. Un des principaux défis à relever à cet égard est celui de la découverte et de la vérification d'éléments pertinents dans un volume sans cesse croissant d'informations mises en ligne, en particulier s'agissant des photos et des vidéos qu'enregistrent les smartphones et les autres appareils mobiles, certains de ces documents pouvant avoir été altérés ou détournés de leur objet réel par de fausses attributions.

Parallèlement, l'émergence des juridictions pénales et des mécanismes d'enquête internationaux, de même que de services nationaux chargés de la répression des crimes de guerre, rend plus pressante encore la nécessité de normes communes régissant l'extraction, la conservation et l'analyse d'informations de sources ouvertes susceptibles d'être produites en preuve dans le cadre de poursuites pénales. Pour que ces informations soient recevables aux fins d'une procédure judiciaire, les procureurs et les conseils doivent habituellement être en mesure d'en attester l'authenticité et de garantir qu'elles ont fait l'objet d'une chaîne de contrôle stricte. De tels éléments ont bien plus de chances d'être utiles aux procureurs et aux conseils s'ils ont été traités et préparés correctement. S'ils ont fait l'objet de méthodes de collecte et de conservation douteuses, par contre, ils ne seront pas considérés comme fiables pour établir les faits dans une affaire. Les tribunaux et les mécanismes d'enquête tireront avantage de l'existence de critères clairs pour apprécier le poids à accorder aux informations de sources ouvertes en tant qu'éléments de preuve tendant à établir le lien entre un crime et son auteur ou la commission du crime lui-même. La normalisation des méthodes d'authentification et de vérification sera tout aussi utile aux missions d'établissement des faits, dont les enquêtes font également une place plus large aux éléments de sources ouvertes numériques. Les commissions d'enquête, les volets des opérations de maintien de la paix consacrés aux droits humains, les bureaux hors siège du Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH) et d'autres activités de surveillance et d'enquête de l'ONU sont tous appelés à bénéficier de principes et d'approches méthodologiques solides venant étayer la validité et le poids de leurs constatations et conclusions.

Pour répondre à ce besoin, nos institutions, le Human Rights Center de la faculté de droit de l'Université de Californie à Berkeley et le HCDH, ont uni leurs ressources pour publier le présent ouvrage, intitulé *Protocole de Berkeley sur l'utilisation de sources ouvertes numériques dans les enquêtes : Guide pratique pour l'utilisation efficace des informations issues de sources ouvertes numériques dans les enquêtes sur les violations du droit pénal international, du droit international des droits humains et du droit international humanitaire*. Le chemin qui a conduit à cette publication trouve son origine sur le campus de Berkeley en 2009, lorsque le Human Rights Center a réuni des experts, des technologues, des journalistes et des militants pour mettre au point des stratégies visant à utiliser des technologies et des méthodes numériques pour faire la lumière sur les violations des droits humains et en recueillir les preuves. Depuis, le Human Rights Center a organisé une série d'ateliers pluridisciplinaires, en collaboration avec un éventail de spécialistes dans les domaines technique, juridique

et méthodologique, issus notamment du HCDH, afin de mettre en commun des idées, de concevoir de nouveaux outils et de cerner et peaufiner des critères, des normes et des méthodes pour découvrir, évaluer, vérifier et préserver des informations de sources ouvertes numériques tendant à établir l'existence d'atteintes aux droits humains, l'objectif étant de faire en sorte que les auteurs de ces actes en répondent devant la justice. Cette démarche était en phase avec les travaux que menait le HCDH pour mettre au point des orientations et des outils destinés à soutenir et à conseiller les commissions d'enquête et les missions d'établissement des faits des Nations Unies ainsi que le personnel du HCDH, qui est de plus en plus souvent amené à recourir à des informations de sources ouvertes pour établir des faits et enquêter.

L'élaboration du Protocole de Berkeley s'est faite grâce aux contributions de collaborateurs d'une grande diversité en termes de parcours professionnel, de contexte juridique et culturel d'origine, de genre et de nationalité. Elle a donné lieu à plus de 150 consultations de spécialistes et a bénéficié de l'apport de parties prenantes de premier plan, notamment des enquêteurs de l'ONU spécialisés dans le domaine des droits humains. Elle s'est également appuyée sur les connaissances approfondies de groupes de travail spécialisés de la Section de la méthodologie, de l'éducation et de la formation du HCDH et du Bureau du Procureur de la Cour pénale internationale. Conformément aux normes internationales, le HCDH et le Human Rights Center ont soumis le Protocole de Berkeley à un rigoureux processus d'examen, de révision et de validation.

Fort de cette approche collaborative, le Protocole de Berkeley contient des normes internationales pour la conduite de recherches en ligne sur les violations présumées du droit international des droits humains, du droit international humanitaire et du droit pénal international, de même qu'il fournit des orientations relatives aux méthodes et aux procédures à appliquer pour garantir que la collecte, l'analyse et la conservation des produits de ces recherches se font de manière professionnelle et dans le respect de la légalité et de la déontologie. Enfin, il expose les mesures que les enquêteurs en ligne peuvent prendre pour protéger leur propre sécurité numérique, physique et psychosociale ainsi que celle des autres personnes concernées que sont notamment les témoins, les victimes et les intervenants de première ligne (par exemple, des citoyens, des militants et des journalistes), qui risquent leur propre bien-être pour recueillir des informations sur des violations des droits humains et des violations graves du droit international.

Le Protocole de Berkeley s'inscrit dans la lignée de deux protocoles antérieurs des Nations Unies : le *Protocole du Minnesota relatif aux enquêtes sur les décès résultant potentiellement d'actes illégaux* (Protocole du Minnesota) (1991, mis à jour en 2016), et le *Manuel pour enquêter efficacement sur la torture et autres peines ou traitements cruels, inhumains ou dégradants* (Protocole d'Istanbul) (1999, mis à jour en 2004). Le Protocole du Minnesota, fruit du travail de juristes et de médecins légistes engagés dans la recherche de personnes disparues dans les années 1980, établit des normes et des procédures internationales pour mener des enquêtes médico-légales sur les décès suspects ou n'ayant pas fait l'objet des diligences voulues, et sert à évaluer la crédibilité de telles enquêtes. Dans le même ordre d'idées, le Protocole d'Istanbul fournit des orientations aux professionnels de la santé et aux juristes appelés à reconnaître et à consigner les séquelles physiques et psychosociales de la torture, de sorte que ces éléments puissent servir à établir des faits en justice ou dans d'autres cadres, comme les enquêtes et la surveillance dans le domaine des droits humains. Les trois protocoles sont fondés sur la conviction que la science, la technologie et le droit peuvent – et doivent – œuvrer de concert au service des droits humains. Comme ses prédécesseurs, le Protocole de Berkeley sera disponible dans les langues officielles

des Nations Unies afin d'en faciliter l'utilisation et d'en accroître l'utilité à l'échelle mondiale.

Nous avons l'espoir que, dans ce monde en pleine transition numérique, le Protocole de Berkeley aidera les enquêteurs en ligne – juristes, défenseurs des droits humains, journalistes ou autres – à mettre au point et employer des procédures efficaces pour recueillir des informations vérifiées et probantes sur des violations du droit international des droits humains, du droit international humanitaire et du droit pénal international, en tirant le meilleur parti des sources ouvertes numériques, de sorte que les responsables de telles violations aient à en répondre dans des procès équitables.

Eric Stover
Directeur académique, Human Rights Center,
faculté de droit de l'Université de Californie
à Berkeley

Michelle Bachelet
Haute-Commissaire des Nations Unies
aux droits de l'homme

Résumé introductif

Les enquêtes en sources ouvertes se fondent entièrement ou partiellement sur des informations accessibles au public pour mener des recherches en ligne à caractère formel et systématique sur des agissements présumés. Aujourd'hui, de grandes quantités d'informations sont disponibles sur Internet, où un paysage numérique en évolution rapide a donné naissance à de nouveaux types et de nouvelles sources d'information qui pourraient s'avérer utiles dans le cadre d'enquêtes menées sur des allégations de violations des droits humains et de graves crimes internationaux. La capacité d'enquêter sur des faits ainsi allégués est d'un intérêt particulier pour les enquêteurs et enquêtrices qui ne sont pas en mesure de se rendre en personne et en temps voulu sur les lieux des crimes, ce qui est souvent le cas pour les enquêtes internationales.

Les informations de sources ouvertes peuvent fournir des pistes, confirmer des éléments issus d'activités de renseignement et servir de preuves directes dans les procédures judiciaires. Cela étant, pour que ces informations soient utilisables dans des cadres formels, comme les enquêtes judiciaires, les missions d'établissement des faits et les commissions d'enquête, les enquêteurs doivent, pour les obtenir, user de méthodes cohérentes qui renforcent la précision de leurs constatations et conclusions, tout en permettant aux juges et à d'autres instances d'établissement des faits de mieux apprécier la qualité du processus d'enquête lui-même. Le *Protocole de Berkeley sur l'utilisation de sources ouvertes numériques dans les enquêtes* a été conçu pour mettre des normes et des orientations internationales à la disposition des enquêteurs qui travaillent dans les domaines de la justice pénale et des droits humains sur le plan international. Les personnes chargées de ces enquêtes proviennent de nombreuses institutions et organisations, qu'il s'agisse d'organes de presse, de groupes de la société civile ou d'organisations non gouvernementales, d'organisations ou de tribunaux internationaux, ou encore d'instances d'enquête nationales ou internationales. L'établissement de normes cohérentes et mesurables à l'appui de ce domaine d'activité pluridisciplinaire est une façon de professionnaliser la pratique des enquêtes en sources ouvertes.

Bien que les directives et les formations relatives à l'utilisation de certains outils et logiciels soient essentielles pour l'amélioration de la qualité des enquêtes en sources ouvertes numériques, le Protocole de Berkeley ne porte pas sur des moyens technologiques, des plateformes, des logiciels ou des outils particuliers, mais plutôt sur des principes et des méthodes sous-jacents qui sont d'application constante, même lorsque la technologie elle-même change. Ces principes énoncent les normes minimales à respecter, du point de vue juridique et déontologique, pour mener efficacement des enquêtes en sources ouvertes. Les enquêteurs qui suivront les orientations fournies par le Protocole de Berkeley assureront la qualité de leur travail tout en réduisant au minimum les risques physiques, psychosociaux et numériques auxquels ils pourraient s'exposer ou exposer autrui.

Le Protocole de Berkeley se veut un outil d'apprentissage et un guide de référence à l'usage des enquêteurs. Il s'ouvre sur un chapitre introductif suivi de trois chapitres consacrés aux cadres généraux, à savoir les principes, les considérations juridiques et la sécurité. Les chapitres restants portent sur le processus d'enquête lui-même. Cette partie débute par un chapitre sur la préparation et la planification stratégique, suivi d'un chapitre sur les différentes étapes d'une enquête – les investigations en ligne, l'appréciation préliminaire, la collecte, la conservation, la vérification, et l'analyse d'enquête. Elle s'achève sur un chapitre consacré à la méthode et aux principes applicables à la communication des résultats de l'enquête en sources ouvertes.

Collaborations et participations

Comité de coordination du Protocole de Berkeley

Lindsay Freeman, chercheuse juridique principale, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Alexa Koenig, Directrice exécutive, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Eric Stover, Directeur académique, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Comité de rédaction du Protocole de Berkeley

Sareta Ashraph, conseillère juridique principale ; avocate, Garden Court Chambers ; anciennement analyste principale, Équipe d'enquêteurs des Nations Unies chargée de concourir à amener Daech/État islamique d'Iraq et du Levant à répondre de ses crimes

Alix Dunn, Directrice exécutive, The Engine Room

Richard Goldstone, anciennement juge, Cour constitutionnelle sud-africaine ; anciennement Procureur du Tribunal pénal international pour l'ex-Yougoslavie et du Tribunal pénal international pour le Rwanda

Brenda J. Hollis, Coprocureure internationale, Chambres extraordinaires au sein des tribunaux cambodgiens ; anciennement Procureure, Tribunal spécial résiduel pour la Sierra Leone

Tanya Karanasios, Directrice des programmes, WITNESS

Enrique Piracés, Directeur des programmes relatifs aux médias et aux droits humains, Center for Human Rights Science, Université Carnegie Mellon

Beth Van Schaack, professeure invitée, enseignante en droits humains, Stanford Law School ; anciennement adjointe de l'Ambassadeur itinérant pour les questions relatives aux crimes de guerre, Bureau de la justice pénale internationale, Département d'État des États-Unis

Michel de Smedt, Directeur, Division des enquêtes, Bureau du Procureur, Cour pénale internationale

Alan Tieger, premier substitut du Procureur, Bureau du Procureur spécialisé pour le Kosovo ; anciennement premier substitut du Procureur, Tribunal pénal international pour l'ex-Yougoslavie

Christian Wenaweser, Représentant permanent du Liechtenstein auprès de l'Organisation des Nations Unies ; anciennement Président, Assemblée des États Parties au Statut de Rome de la Cour pénale internationale

Alex Whiting, chef des enquêtes, Bureau du Procureur spécialisé pour le Kosovo ; professeur praticien, Harvard Law School ; anciennement coordonnateur des poursuites et coordonnateur des enquêtes, Bureau du Procureur, Cour pénale internationale

Susan Wolfinbarger, spécialiste des affaires étrangères et responsable de l'Équipe d'analyse des données, Département d'État des États-Unis ; anciennement directrice de projet principale, Projet des technologies géospatiales, Association américaine pour le progrès de la science

Comité consultatif du Protocole de Berkeley

Federica D'Alessandra, Directrice exécutive, Programme d'Oxford sur la paix et la sécurité internationales, Université d'Oxford ; rédactrice, *Handbook on Civil Society Documentation of Serious Human Rights Violations: Principles & Best Practices*, Public International Law and Policy Group

Stuart Casey-Maslen, professeur honoraire, faculté de droit, Université de Pretoria ; collaborateur, *Protocole du Minnesota sur les décès résultant potentiellement d'actes illégaux* (2016)

Alison Cole, conseillère spécialisée en droits humains, Direction des affaires intérieures, Nouvelle-Zélande

Françoise Hampson, professeure émérite, University of Essex School of Law ; membre de la Commission d'enquête sur le Burundi

Christof Heyns, professeur de droit des droits humains, Université de Pretoria ; membre du Comité des droits de l'homme ; anciennement Rapporteur spécial sur les exécutions extrajudiciaires, sommaires ou arbitraires ; coordonnateur, *Protocole du Minnesota sur les décès résultant potentiellement d'actes illégaux* (2016)

Vincent Iacopino, conseiller médical principal, Physicians for Human Rights ; collaborateur principal, *Manuel pour enquêter efficacement sur la torture et autres peines ou traitements cruels, inhumains ou dégradants* (Protocole d'Istanbul)

Kelly Matheson, avocat principal et directeur de programme, WITNESS ; auteur, Video as Evidence Field Guide

Hanny Megally, Commissaire, Commission d'enquête internationale indépendante sur la République arabe syrienne ; maître de recherche, Center on International Cooperation, New York University

Juan Méndez, professeur en résidence de droit des droits humains, Washington College of Law ; anciennement Rapporteur spécial sur la torture et autres peines ou traitements cruels, inhumains ou dégradants ; coordonnateur, protocole universel sur les entretiens d'enquête et les garanties associées

Aryeh Neier, Président émérite, Open Society Foundations

Navi Pillay, Présidente, Commission internationale contre la peine de mort ; anciennement Haute-Commissaire des Nations Unies aux droits de l'homme ; anciennement juge, Cour pénale internationale ; anciennement Présidente, Tribunal pénal international pour le Rwanda

Paulo Sérgio Pinheiro, Président, Commission d'enquête internationale indépendante sur la République arabe syrienne ; anciennement Rapporteur spécial sur la situation des droits de l'homme au Burundi ; anciennement Rapporteur spécial sur la situation des droits de l'homme au Myanmar

Thomas Probert, maître de conférences extraordinaire, Centre for Human Rights, Université de Pretoria ; chargé de recherche, Centre of Governance and Human Rights, Université de Cambridge ; collaborateur, *Protocole du Minnesota sur les décès résultant potentiellement d'actes illégaux* (2016)

Stephen Rapp, membre éminent, Simon-Skjodt Center for the Prevention of Genocide, United States Holocaust Memorial Museum ; anciennement Ambassadeur itinérant pour les questions relatives aux crimes de guerre, Bureau de la justice pénale internationale, Département d'État des États-Unis ; anciennement Procureur, Tribunal spécial pour la Sierra Leone

Cristina Ribeiro, coordinatrice des enquêtes, Bureau du Procureur, Cour pénale internationale

Patricia Sellers, conseillère spéciale du Bureau du Procureur pour les questions relatives au genre, Cour pénale internationale ; chercheuse invitée, Kellogg College, Université d'Oxford ; anciennement conseillère juridique et substitute du Procureur, Tribunal pénal international pour l'ex-Yougoslavie et Tribunal pénal international pour le Rwanda

Participants et participantes

Workshop on the New Forensics: Using Open Source Information to Investigate Grave Crimes (Atelier sur la criminalistique nouvelle : l'utilisation des informations de sources ouvertes pour enquêter sur les crimes graves) – Bellagio (Italie), 2017

Hadi Al Khatib, Syrian Archive

Stuart Casey-Maslen, Université de Pretoria

Yvan Cuypers, Cour pénale internationale

Scott Edwards, Amnesty International

Lindsay Freeman, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Alexa Koenig, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Steve Kostas, Open Society Justice Initiative

Andrea Lampros, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Kelly Matheson, WITNESS

Félim McMahon, Cour pénale internationale

Julian Nicholls, Cour pénale internationale

Thomas Probert, Université de Cambridge

Cristina Ribeiro, Cour pénale internationale

Gavin Sheridan, Vizlegal

Eric Stover, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Alan Tieger, Tribunal pénal international pour l'ex-Yougoslavie

Mark Watson, Commission pour la justice internationale et la responsabilité

Guy Willoughby, The Association for the Study of War Crimes

Workshop on Building an Ethical Framework for Open Source Investigations (Atelier sur l'élaboration d'un cadre déontologique pour les enquêtes en sources ouvertes) – Université d'Essex (Royaume-Uni), 2019

Fred Abrahams, Human Rights Watch

Leenah Bassouni, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Federica D'Alessandra, Université d'Oxford

Sam Dubberley, Amnesty International

Jennifer Easterday, JustPeace Labs

Scott Edwards, Amnesty International

Lindsay Freeman, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Geoff Gilbert, Université d'Essex

Christopher « Kip » Hale, Commission pour la justice internationale et la responsabilité

Evanna Hu, Omelas

Gabriela Ivens, titulaire de bourse Mozilla ; WITNESS

Alexa Koenig, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Matt Mahmoudi, Université de Cambridge

Lorna McGregor, Université d'Essex

Daragh Murray, Université d'Essex

Vivian Ng, Université d'Essex

Enrique Piracés, Center for Human Rights Science, Carnegie Mellon University

Zara Rahman, The Engine Room

Sasha Robehmed, The Engine Room

Ilia Siatitsa, Privacy International

Représentant ou représentante du HCDH, Section de la méthodologie, de l'éducation et de la formation

Round Table on Legal Issues Arising from Open Source Investigations (Table ronde sur les questions juridiques soulevées par les enquêtes en sources ouvertes) – La Haye, 2019

David Akerson, Équipe d'enquêteurs des Nations Unies chargée de concourir à amener Daech/État islamique d'Iraq et du Levant à répondre de ses crimes

Sareta Ashraph, Garden Court Chambers

Danya Chaikel, Bureau du Procureur spécialisé pour le Kosovo

Alan Clark, Cour pénale internationale

Federica D'Alessandra, Université d'Oxford

Nico Dekens, Bellingcat

Chris Engels, Commission pour la justice internationale et la responsabilité

Lindsay Freeman, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Emma Irving, Université de Leiden

Michelle Jarvis, Mécanisme international, impartial et indépendant chargé de faciliter les enquêtes sur les violations les plus graves du droit international commises en République arabe syrienne depuis mars 2011 et d'aider à juger les personnes qui en sont responsables

Edward Jeremy, Cour pénale internationale

Ashley Jordana, Global Rights Compliance

Sang-Min Kim, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Alexa Koenig, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Nicholas Koumjian, Mécanisme d'enquête indépendant pour le Myanmar

Bastiaan Van Der Laaken, Mécanisme international, impartial et indépendant chargé de faciliter les enquêtes sur les violations les plus graves du droit international commises en République arabe syrienne depuis mars 2011 et d'aide à juger les personnes qui en sont responsables

Dearbhla Minogue, Global Legal Action Network

Nick Ortiz, Université de Leiden

Matevz Pezdirc, réseau génocide de l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale

Sanja Popovic, Bureau du Procureur spécialisé pour le Kosovo

Steven Powles, Doughty Street Chambers ; Comité sur les crimes de guerre, Association internationale du barreau

Stephen Rapp, Simon-Skjodt Center for the Prevention of Genocide, United States Holocaust Memorial Museum

Cristina Ribeiro, Cour pénale internationale

Mark Robson, Commission pour la justice internationale et la responsabilité

Brad Samuels, SITU Research

Dalila Seoane, Civitas Maxima

Carsten Stahn, Université de Leiden

Melinda Taylor, Cour pénale internationale

Alan Tieger, Bureau du Procureur spécialisé pour le Kosovo

Raquel Vázquez Llorente, eyeWitness to Atrocities

Expertes et experts supplémentaires ayant pris part à l'examen

Elise Baker, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Sean Brooks, Center for Long-Term Cybersecurity, Université de Californie à Berkeley

Stephanie Croft, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Sam Dubberley, Amnesty International

Thomas Ewing, The Center for Advanced Defense Studies

Christopher « Kip » Hale, Commission pour la justice internationale et la responsabilité

Gabriela Ivens, Human Rights Watch

Felim McMahon, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Daragh Murray, Université d'Essex

Yvonne Ng, WITNESS

Zara Rahman, The Engine Room

Mark Robson, Commission pour la justice internationale et la responsabilité

Justin Seitz, Hunchly

Andrea Trewinnard, Human Rights Center, faculté de droit de l'Université de Californie à Berkeley

Steve Trush, Center for Long-Term Cybersecurity, Université de Californie à Berkeley

Raquel Vázquez Llorente, eyeWitness to Atrocities

Mentions spéciales

Des remerciements particuliers sont adressés aux membres du groupe de travail sur les enquêtes en ligne du Bureau du Procureur de la Cour pénale internationale.

Une mention est également due aux nombreux collègues au sein du HCDH dont les efforts ont permis la réalisation de cette publication commune*.

* Conformément à la politique du HCDH, les contributions des fonctionnaires du Haut-Commissariat à ses publications ne sont pas attribuées.

Abréviations

CICR	Comité international de la Croix-Rouge
HCDH	Haut-Commissariat des Nations Unies aux droits de l'homme
HTML	langage de balisage hypertexte
IP	protocole Internet
ONG	organisation non gouvernementale
ONU	Organisation des Nations Unies
PDF	format de document portable
URI	identificateur uniforme de ressources
URL	localisateur uniforme de ressources
VPN	réseau privé virtuel

1

INTRODUCTION

SOMMAIRE DU CHAPITRE

- Objet
- Public
- Définitions

1. Le Protocole de Berkeley sur l'utilisation des sources ouvertes dans les enquêtes expose les normes professionnelles qui devraient être appliquées à la recherche, la collecte, la conservation, l'analyse et la présentation des informations de sources ouvertes numériques, et à leur utilisation dans les enquêtes relevant du droit pénal international et du droit international des droits humains. Les informations de sources ouvertes sont de celles que tout membre du public peut consulter, acquérir ou demander, sans devoir faire état d'une qualité juridique particulière ni recourir à un accès non autorisé. Les informations de sources ouvertes numériques sont accessibles au public sous forme numérique ; elles proviennent généralement d'Internet. Constituées de données générées par les utilisateurs ou par les machines, elles comprennent, par exemple, des contenus publiés sur les médias sociaux, des documents, images, enregistrements vidéo et audio mis en ligne sur des sites Web ou sur des plateformes de partage d'informations, des images satellites et des données publiées par les autorités publiques[1]. Les enquêtes en sources ouvertes numériques sont des enquêtes fondées sur des informations de sources ouvertes numériques. Pour alléger le texte, il sera simplement question, dans le présent Protocole, de « sources ouvertes » pour désigner les « sources ouvertes numériques » concernées par ces informations et ces enquêtes.

2. Si le recours aux informations de sources ouvertes pour mener des enquêtes n'est pas une nouveauté, le volume et la diversité de ces sources a augmenté en raison de l'utilisation sans cesse croissante d'Internet et d'autres ressources numériques pour échanger des informations, comme l'atteste notamment la prolifération des médias sociaux. Le Protocole porte à la fois sur les complications propres à l'exploitation des informations numériques et sur le défi que représente l'appréciation des sources et la vérification des informations disponibles dans les espaces ouverts en ligne.

3. Alors qu'un nombre croissant d'enquêteurs dans les domaines du droit pénal international et des droits humains internationaux se tournent vers Internet pour faciliter leur travail, il n'existe pas de références, de directives ou de normes universellement admises pour guider les enquêtes en sources ouvertes. Le Protocole entend combler cette lacune en formulant des principes et des pratiques qui aideront les enquêteurs à mener leurs activités à un niveau professionnel et, le cas échéant, qui favoriseront la conservation d'informations de sources ouvertes qui pourraient servir à des mécanismes d'attribution des responsabilités.

4. Le Protocole met un accent particulier sur les enquêtes en sources ouvertes menées en faveur de la justice et de l'établissement des responsabilités au niveau international. En termes généraux, ces enquêtes se répartissent comme suit : la consignation et la conservation d'informations, la collecte d'éléments de preuve et l'établissement de faits touchant aux droits humains ; les enquêtes menées par les commissions d'enquête et les missions d'établissement des faits[2] ; d'autres types de recherches et d'enquêtes menées en exécution de mandats internationaux[3] ; les processus de paix et de réconciliation ; les litiges civils ; les procès pénaux, y compris les procédures pénales internationales. Comme les enquêtes

1 Cette liste n'est pas exhaustive.

2 Les commissions d'enquête et les missions d'établissement des faits sont des organes créés par des gouvernements ou des organisations internationales afin d'examiner diverses questions. Elles rendent des constatations, dégagent des conclusions juridiques et font des recommandations. Les résultats des travaux des commissions et des missions internationales, quoique non contraignants légalement parlant, peuvent avoir une influence considérable. Dans certaines juridictions, les constatations et conclusions des commissions d'enquête nationales peuvent être contraignantes au regard de la loi. Pour plus d'informations sur les commissions d'enquête et les missions d'établissement des faits internationales, voir Conseil des droits de l'homme, « Commissions d'enquête et missions d'établissement des faits ». Disponible à l'adresse www.ohchr.org/fr/hr-bodies/hrc/co-is.

3 Voir, par exemple, le rapport de la Haute-Commissaire des Nations Unies aux droits de l'homme sur la situation des droits de l'homme en République bolivarienne du Venezuela (A/HRC/41/18), soumis en application de la résolution 39/1 du Conseil des droits de l'homme. Voir aussi la résolution 41/2, dans laquelle le Conseil des droits de l'homme a prié la Haute-Commissaire d'établir un rapport sur la situation des droits de l'homme aux Philippines.

en responsabilités[4], les exigences retenues dans le Protocole quant aux méthodes employées et aux informations collectées peuvent s'avérer plus contraignantes que celles auxquelles sont soumis d'autres domaines, comme le journalisme et la défense des droits de l'homme. Quelle que soit la finalité de leurs investigations, s'ils adhèrent aux principes méthodologiques énoncés dans le Protocole, qui sont fondés sur des normes juridiques éprouvées, les enquêteurs en sources ouvertes livreront un travail de qualité qui présentera la plus grande utilité possible pour les juridictions ou autres instances qui en feraient usage dans un processus d'établissement des responsabilités.

5. L'accent est également mis, dans le Protocole, sur les enquêtes en matière de violations du droit international, notamment les violations des droits humains, et de violations du droit pénal international, notamment les crimes de guerre, les crimes contre l'humanité et le génocide. Qui plus est, les orientations fournies par le Protocole peuvent s'appliquer à d'autres types d'enquêtes, notamment dans le cadre de poursuites engagées devant des juridictions nationales ou locales.

6. En définitive, le Protocole est conçu pour aider les enquêteurs et les enquêtrices à mener leurs activités selon une méthodologie professionnelle qui s'accorde largement avec les exigences juridiques et les normes déontologiques. Il a également pour vocation d'aider divers utilisateurs finals du processus d'enquête, dont les avocats, les juges et d'autres décideurs, à mieux comprendre et apprécier les techniques d'investigation en sources ouvertes. Il se veut à la fois ressource pour le praticien chevronné et outil de formation et d'apprentissage pour celle ou celui qui souhaite apprendre à enquêter sur des violations présumées du droit international en faisant appel à des sources ouvertes[5].

A. Objet

7. Cela fait longtemps que les enquêteurs vont puiser dans les sources ouvertes. L'exploitation systématique de ces terrains d'investigation a toutefois connu un essor entre le début et le milieu du XX^{e} siècle, avec un intérêt particulier pour l'extraction de renseignements contenus dans des émissions de radio et des journaux étrangers[6]. Avec l'apparition du Web pendant les années 1990, suivie par la popularisation des médias sociaux et des téléphones intelligents dans les années 2000, la quantité et la qualité des informations de sources ouvertes ont connu une profonde mutation. Aujourd'hui, quiconque dispose d'un smartphone et d'un accès à Internet peut créer des contenus numériques et les diffuser de par le monde, quoique à des degrés de qualité, de véracité et transparence variables. La croissance du volume des données et de la vitesse à laquelle elles sont transmises ont ouvert aux enquêteurs en sources ouvertes de nouvelles possibilités de collecte et d'analyse d'informations concernant la commission de crimes internationaux et de violations des droits humains. Avec comme corollaire qu'il est devenu relativement aisé pour les créateurs de contenus de faire œuvre de désinformation et de manipuler les données. Le Protocole tente de répondre à la nouveauté de cet environnement et à la complexité des possibilités et des difficultés qui lui sont propres.

8. Les informations de sources ouvertes peuvent s'avérer utiles dans une grande variété d'enquêtes, mais leur rôle est particulièrement critique lorsqu'il s'agit d'enquêter sur des crimes internationaux et des violations des droits humains internationaux. Il y a à cela plusieurs raisons. Premièrement, la conduite des enquêtes procédant d'un mandat international, dont celles menées par les commissions

[4] Des informations de sources ouvertes ont ainsi été utilisées par la mission internationale indépendante d'établissement des faits sur le Myanmar, en même temps que d'autres provenant notamment de sources de première main. Elles ont servi aux vérifications, constatations et conclusions de la mission, dont le rapport final (A/HRC/42/50) a été un des facteurs qui ont conduit le Conseil des droits de l'homme à établir le Mécanisme d'enquête indépendant pour le Myanmar, chargé de mener des enquêtes judiciaires. La mission avait également pour mandat de confier ses informations au Mécanisme, y compris celles provenant de sources ouvertes. Ses rapports ont également servi à étayer l'instance introduite par la Gambie contre le Myanmar, devant la Cour internationale de Justice, pour violation de la Convention pour la prévention et la répression du crime de génocide. Des informations recueillies à une fin donnée peuvent donc, en fin de compte, servir à un autre processus d'établissement des responsabilités.

[5] Le Protocole présente également des modèles pour les enquêtes en sources ouvertes, et un glossaire (voir chap. VIII ci-dessus).

[6] Nikita Mehandru et Alexa Koenig, « ICTs, social media, & the future of human rights », Duke Law & Technology Review, vol. 17, n° 1, p. 129.

d'enquête et les missions d'établissement des faits des Nations Unies, ou celles autorisées par la Cour pénale internationale, est conditionnée par des processus juridiques et politiques[7]. Elles ont donc souvent lieu bien après les faits. Deuxièmement, les enquêtes internationales ne sont souvent pas en mesure de se rendre sur les lieux physiques où les faits sous enquête se sont produits, par exemple, lorsque l'État concerné refuse de coopérer ou d'accorder l'accès. Troisièmement, même lorsque l'autorisation est accordée de se rendre dans une région ou un territoire, les enquêteurs et enquêtrices peuvent n'avoir qu'un accès limité au lieu effectif, ou encore être empêchés d'enquêter sur place ou d'avoir des entretiens en personne, en raison de préoccupations de protection. Quatrièmement, comme la plupart des enquêteurs n'exercent pas les pleins pouvoirs de police sur les territoires dans lesquels les crimes ou les violations auraient été commis, ils peuvent se trouver dans l'impossibilité de recueillir les informations nécessaires. Même dans les cas où il y a coopération de l'État, la dimension transfrontalière de la collecte d'éléments peut en faire un processus ardu, ralenti par de lourdes formalités administratives. Autant de facteurs qui attestent de la valeur et de la nécessité des techniques d'enquête en sources ouvertes qui peuvent se mener au moment des faits et à distance.

9. Le Protocole s'adresse à un groupe varié d'enquêteurs travaillant dans différents contextes, avec des mandats, des pouvoirs d'enquête et des ressources variables. L'approche se doit donc d'être flexible. Il ne s'agit pas de présumer que les personnes qui enquêtent vont effectuer leurs travaux à l'identique, mais de prévoir qu'elles vont devoir, au contraire, adapter leurs méthodes aux particularités de chaque environnement dans lequel elles seront appelées à travailler. En outre, dès lors que les moyens technologiques, les outils et les techniques qui sont mis à contribution dans les enquêtes en sources ouvertes sont en constante évolution, le Protocole ne porte pas sur des outils, plateformes, sites Web, logiciels ou sources en particulier, car ce sont des réalités changeantes, mais sur les principes et les procédures sous-jacents qui devraient guider les enquêtes en sources ouvertes.

10. Le Protocole est conçu pour normaliser les procédures et fournir des orientations méthodologiques qui aident les enquêteurs en sources ouvertes, compte tenu de l'hétérogénéité des enquêtes, des institutions et des juridictions concernées, à comprendre l'importance des précautions suivantes :

    a) Établir la provenance des contenus en ligne et les attribuer à leur source originelle, dans la mesure du possible ;

    b) Évaluer la crédibilité et la fiabilité des sources en ligne ;

    c) Vérifier les contenus en ligne et évaluer leur véracité et leur fiabilité ;

    d) Se conformer aux prescriptions légales et aux normes déontologiques ;

    e) Réduire tout risque ou tout dommage auquel eux-mêmes, leur organisation ou des tiers pourraient être exposés ;

    f) Renforcer la protection des droits humains des sources, y compris leur droit à la vie privée.

B. Public

11. Le public visé par le Protocole est constitué des individus et des organisations qui recherchent, collectent, préservent ou analysent des informations de sources ouvertes afin d'enquêter sur des crimes internationaux ou des violations des droits humains internationaux afin que justice soit faite et que les responsabilités soient établies. Il s'adresse ainsi aux enquêteurs, aux juristes, aux archivistes et aux analystes qui travaillent pour des juridictions internationales, régionales et hybrides, pour des services nationaux chargés de la répression des crimes de guerre, pour des commissions d'enquête, des missions d'établissement des faits, des mécanismes

[7] Des commissions d'enquête et des missions d'établissement des faits mandatées par l'ONU ont été créées par le Conseil de sécurité, l'Assemblée générale, le Conseil des droits de l'homme et le Secrétaire général, entre autres. Le Bureau du Procureur de la Cour pénale internationale enquête à la demande d'États parties ou du Conseil de sécurité, ou, moyennant l'autorisation des juges, de sa propre initiative.

d'enquête indépendants, des organisations internationales, des mécanismes de justice transitionnelle et des organisations non gouvernementales (ONG). Il peut également s'avérer utile aux personnes qui travaillent pour des mécanismes internationaux et régionaux qui mènent des enquêtes judiciaires et quasi judiciaires, en sources ouvertes, sur des violations du droit international[8]. Le Protocole peut également avoir une valeur instructive pour les intervenants numériques de première ligne, tels que des organisations locales ou des chercheurs indépendants qui sont souvent les premiers à publier des constatations et des conclusions fondées sur des informations de sources ouvertes, et dont le travail contribue souvent de façon cruciale à la mise sur pied d'enquêtes en sources ouvertes officiellement mandatées. Le public cible du Protocole comprend aussi des particuliers et des organisations qui aident les victimes à porter plainte au civil contre des auteurs individuels ou des États. Le Protocole peut aussi être utile, de façon générale, à celles et ceux qui dégagent des constatations de fait ou des conclusions de droit à partir d'enquêtes en sources ouvertes, en leur donnant les moyens de mieux apprécier les résultats de ces enquêtes sur lesquels ils se fondent ou portent une appréciation.

12. Cette utilité peut encore s'étendre aux fournisseurs de services en ligne, tels que les plateformes de médias sociaux, qui stockent de grands volumes de données et peuvent jouer un rôle de premier plan dans la préservation des données, ainsi qu'aux concepteurs qui fournissent les logiciels qui viennent renforcer les techniques et procédures d'enquête en sources ouvertes.

C. Définitions

13. Pour que les enquêtes en sources ouvertes soient dotées de normes et d'orientations pratiques, il importe que certains termes soient compris de la même façon par les personnes qui se chargent de ces enquêtes. Les termes utilisés dans l'ensemble du Protocole sont précisés dans la présente section, et notamment les distinctions à opérer entre des termes habituellement confondus[9].

1. Informations de sources ouvertes et de sources fermées

14. Les informations de sources ouvertes sont des informations que tout membre du public peut consulter, acquérir ou demander, sans devoir faire état d'une qualité juridique particulière ni recourir à un accès non autorisé. Les informations de sources fermées sont des informations d'accès limité ou d'accès protégé par la loi[10], mais qui peuvent être obtenues légalement, par voie privée, notamment dans le cadre d'un processus judiciaire, ou remises volontairement. Bien que la définition soit simple, déterminer ce qui relève de la catégorie des informations de sources ouvertes s'avère plus compliqué qu'il n'y paraît lorsqu'il est question de contenus numériques. On trouve sur Internet un volume croissant de données qui ont été divulguées sans le consentement de leurs auteurs. Il peut notamment s'agir d'informations qui ont été piratées, qui ont fait l'objet de fuites, qui ont été révélées en raison de vulnérabilités en matière de sécurité ou qui ont été mises en ligne par une tierce partie sans les permissions voulues. Bien que ces informations soient à la disposition du public, et donc techniquement considérées comme issues de sources ouvertes, certaines de leurs utilisations finales peuvent tomber sous le coup de restrictions juridiques ou déontologiques. Par ailleurs, certaines informations numériques peuvent être obtenues par des personnes qui, grâce à leurs compétences ou formations spécialisées, peuvent accéder à des réseaux et à des données qui ne sont pas ou guère accessibles à l'utilisateur moyen[11]. C'est notamment le cas des informations qui ne peuvent se trouver que

8 Voir, par exemple, les communications et les rapports de visites des titulaires de mandat au titre des procédures spéciales du Conseil des droits de l'homme, à l'adresse www.ohchr.org/fr/special-procedures-human-rights-council. Voir aussi les activités du comité des sanctions créé par le Conseil de sécurité, à l'adresse www.un.org/securitycouncil/fr/content/repertoire/sanctions-and-other-committees.

9 Pour une compilation plus exhaustive des termes et définitions concernés, voir chap. VIII ci-dessous.

10 Par exemple, les informations privilégiées et classifiées.

11 Certains actes peuvent enfreindre les conditions d'utilisation d'un site Web sans être illégaux pour autant, comme l'extraction non autorisée de données qui peut être un motif d'exclusion du site.

sur le dark Web, cette partie d'Internet que seuls peuvent pénétrer certains logiciels, comme le navigateur Tor[12]. L'anonymat assuré par le dark Web le rend attrayant pour les activités illégales. L'utilisation du navigateur Tor et les recherches sur le dark Web n'en sont pas moins légales dans la plupart des pays. Le Protocole classe les informations ainsi obtenues dans la sphère des « sources ouvertes », pour autant qu'il ne soit pas question d'accès non autorisé aux informations. La distinction la plus claire est que les informations de sources ouvertes sont obtenues sans qu'il faille s'adresser ou en faire la demande à des utilisateurs individuels d'Internet[13]. Le fait d'obtenir des informations d'autres utilisateurs d'Internet, en communiquant avec ceux-ci, revient à recourir à des sources fermées.

15. Les informations de sources ouvertes numériques[14] sont des informations de sources ouvertes sur Internet qui sont disponibles, par exemple, sur des sites Web publics, dans des bases de données en ligne ou sur des plateformes de médias sociaux. La section suivante est consacrée aux différentes façons d'obtenir des informations de sources ouvertes.

2. Obtention des informations de sources ouvertes

a) Observation

16. Les contenus de nombreuses plateformes en ligne s'obtiennent simplement en se rendant sur le site concerné au moyen d'un navigateur gratuit. Pour d'autres plateformes, il faut se connecter ou s'inscrire afin d'accéder aux contenus et de les consulter. Ces contenus sont considérés comme d'origine ouverte dès lors que la marche à suivre pour y accéder est à la disposition de tous les utilisateurs dans les juridictions où cet accès est légal, et qu'il n'est pas nécessaire de forcer des contrôles de confidentialité ou de sécurité pour y accéder ou les consulter. Cela étant, certains contenus qui répondent à ces critères peuvent toutefois ne pas être considérés comme étant de sources ouvertes, notamment lorsque les informations concernées sont privilégiées, classifiées ou protégées par la loi d'une autre façon. Dans ces cas, bien que les informations soient consultables par tout un chacun, leur utilisation en tant qu'éléments de preuve dans une procédure judiciaire peut être limitée. Le recours à de tels éléments peut aussi soulever des questions de déontologie ou de méthodologie, lorsque, par exemple, il n'est pas possible de les attribuer ou de les vérifier.

b) Acquisition

17. Plusieurs sources de données utiles aux enquêtes en sources ouvertes se trouvent sur des plateformes payantes ou mixtes. Dans ce second cas, deux modèles sont proposés, l'un gratuit et l'autre supérieur, lequel offre, moyennant paiement, des fonctionnalités et des données supplémentaires. Les entreprises qui recueillent et organisent des données publiques et offrent des services gratuits ou payants pour y accéder se font plus nombreuses. Une quantité importante d'informations utiles aux enquêteurs en sources ouvertes se trouvent dans des bases de données ou sur des plateformes dotées d'un verrou d'accès payant. Aux fins du Protocole, les informations de sources ouvertes s'entendent également de celles qui proviennent de services à péage utilisables par tout membre du public, mais non de services dont l'utilisation est limitée à certains groupes, comme les membres des forces de l'ordre ou les enquêteurs privés agréés.

c) Demande

18. Dans le présent contexte, le terme « demande » renvoie à des demandes qui peuvent être soumises par toute personne en vue d'obtenir des informations publiques auprès des organismes publics en vertu de la liberté d'information ou des lois relatives à l'accès à l'information. Il ne s'entend pas des demandes adressées à des personnes, des entreprises ou des organisations pour obtenir qu'elles fournissent

[12] Le dark Web est la partie d'Internet que seuls peuvent pénétrer certains logiciels spécialisés, dont le navigateur Tor est un exemple.

[13] Il faut certes une certaine interaction en ligne pour acquérir des informations auprès d'une base de données privée ou pour adresser une demande d'informations à un organisme public, mais ces processus sont souvent automatiques et distincts des interactions avec d'autres utilisateurs d'Internet dont il est question ici.

[14] Les informations de sources ouvertes peuvent aussi être appelées contenus, éléments ou données en ligne dans le Protocole.

à titre volontaire des informations dont elles disposent, mais désigne exclusivement les demandes soumises aux organismes publics qui sont légalement obligés de répondre de la même façon à tout un chacun. Les enquêtes en sources ouvertes peuvent conduire à d'autres activités d'investigation en ligne, comme le fait de prendre contact avec des sources externes au moyen de services de messagerie, dans le cadre de groupes de discussion et de forums, ou par voie de courriel. De telles démarches dépassent le cadre des enquêtes visées par le Protocole.

3. Renseignement de sources ouvertes

19. Le renseignement tiré du domaine public est une sous-catégorie des informations de sources ouvertes. Il a pour finalité d'éclairer les orientations à suivre et les décisions à prendre, le plus souvent dans les domaines militaire ou politique. Alors que les informations de sources ouvertes comprennent toutes les informations publiques que quiconque peut obtenir légalement, les exploitées et diffusées en temps utile à un public approprié afin de répondre à un besoin de renseignement particulier »[15]. Pour ce qui concerne les affaires relatives à des crimes internationaux et des violations des droits humains internationaux, le renseignement de sources ouvertes sert à éclairer la prise de décisions concernant, par exemple, les activités de sécurité, comme la protection des témoins et du personnel de terrain ou la localisation de personnes qui présentent un intérêt pour les affaires, mais n'intervient pas dans la collecte d'informations menée dans le cadre des enquêtes, notamment aux fins de l'établissement des éléments de divers crimes.

4. Enquête en sources ouvertes

20. L'enquête en sources ouvertes concerne le recours à des sources ouvertes pour réunir des informations – et des éléments de preuve.

5. Preuves provenant de sources ouvertes

21. Les termes « élément de preuve » et « preuve » sont à distinguer du terme « information »[16]. Les premiers sont généralement définis, dans l'ensemble des juridictions, comme des éléments tendant à établir les faits concernés par une enquête ou une instance judiciaires, telle un procès. Les éléments de preuve provenant de sources ouvertes sont des informations de sources ouvertes qui ont une valeur probante et peuvent être reçues en preuve afin d'établir des faits dans une procédure judiciaire. Il importe de ne pas faire un usage erroné ou trop fréquent des termes « preuve » et « élément de preuve » lorsqu'il est question d'« informations » au sens général.

6. Informations de sources ouvertes et logiciels libres

22. On emploie souvent les termes « libre » ou « open source » pour qualifier un logiciel ou un programme qui peuvent être utilisés et republiés librement, sans restrictions liées aux droits d'auteurs, aux brevets ou à d'autres contrôles légaux. Le logiciel libre est conçu à partir d'un code source que toute personne disposant de l'accès voulu peut inspecter, modifier et perfectionner[17]. Les utilisateurs moyens ne le voient généralement pas, mais il peut être ajusté et adapté par des programmeurs. Si les logiciels libres sont donc à distinguer des informations de sources ouvertes, ils sont souvent utilisés, comme d'autres outils d'utilisation libre, pour trouver, collecter, préserver et analyser des informations de sources ouvertes.

7. Crédibilité et fiabilité

23. Lorsqu'un élément de preuve testimoniale est produit à un procès pénal international, les juges apprécient « la crédibilité du témoin » et « la fiabilité de son témoignage »[18]. Selon les orientations établies à l'intention des commissions d'enquête, des missions

[15] National Open Source Enterprise, Intelligence Community Directive n° 301, 11 juillet 2006, p. 8 (notes de bas de page omises).

[16] Federica D'Alessandra *et al.*, dir., *Manuel pour la documentation de la société civile sur les violations graves des droits de l'homme : Principes et meilleures pratiques* (La Haye, Public International Law and Policy Group, 2016), p. 18.

[17] Voir Opensource.com, « What is open source? ».

[18] Cour pénale internationale, *Le Procureur c. Bosco Ntaganda*, affaire n° ICC-01/04-02/06, jugement du 8 juillet 2019, par. 53.

d'établissement des faits et des autres enquêteurs similairement mandatés par l'ONU, « l'enquêteur doit évaluer la crédibilité et la fiabilité de la personne interrogée »[19]. Il est précisé que cette « évaluation consiste à se demander si les informations présentent un intérêt pour l'objet de l'enquête. Elle porte également sur la fiabilité des sources et sur la validité ou la véracité des informations »[20].

Ces termes sont utilisés comme suit aux fins du présent Protocole :

a) La « crédibilité » renvoie à la qualité qui permet d'être cru ou digne de foi ;

b) La « fiabilité » renvoie à la capacité d'être constant, sûr ou prévisible ;

c) La « véracité » ou la « validité » renvoient à l'exactitude, la fidélité ou la conformité par rapport au fait rapporté.

[19] HCDH, *Commissions d'enquête et missions d'établissement des faits sur le droit international des droits de l'homme et le droit humanitaire international : Orientations et pratiques* (New York et Genève, 2015), p. 58. Disponible à l'adresse https://www.ohchr.org/sites/default/files/Documents/Publications/CoI_Guidance_and_Practice_FR.pdf.

[20] Ibid., p. 59.

II

PRINCIPES

SOMMAIRE DU CHAPITRE

- Pour respecter les principes professionnels relatifs aux enquêtes en sources ouvertes, les enquêteurs doivent veiller à être comptables, compétents et objectifs, et à ce que leurs travaux s'effectuent conformément à la loi et compte dûment tenu des considérations de sécurité.
- Les enquêteurs doivent également être attentifs aux méthodes utilisées à tous les stades du cycle de vie de leurs enquêtes. Les principes méthodologiques à respecter sont, au minimum, l'exactitude, la minimisation des données, la conservation des données et la sécurité dès la conception.
- Enfin, tous les enquêteurs devraient être guidés par des considérations d'ordre déontologique. Il s'agit, au minimum, de protéger la dignité de toutes les personnes qui prennent part à une enquête ou sont visées par celle-ci, et de faire preuve d'humilité, d'inclusivité, d'indépendance et de transparence.

24. Si les moyens technologiques, les outils et les techniques utilisés dans les enquêtes en sources ouvertes sont appelés à changer, certains grands principes méthodologiques et déontologiques devraient, quant à eux, rester inchangés. La définition de ces principes est une étape importante vers la professionnalisation des activités d'enquête en sources ouvertes. Les principes suivants sont des gages fondamentaux de la qualité de ces enquêtes, qui leur permettront de gagner en crédibilité et en fiabilité, et en accroîtront l'utilité potentielle s'agissant d'assurer l'application du principe de responsabilité et de réduire au minimum le tort qui pourrait être fait à diverses parties prenantes.

A. Principes professionnels

1. Responsabilité

25. Les enquêteurs en sources ouvertes doivent pouvoir être tenus responsables de leurs actes. C'est généralement le cas si des méthodes claires régissent la collecte de documents, la consignation par écrit des activités menées et leur contrôle. La transparence des méthodes et des procédures d'enquête est un élément essentiel de la bonne application du principe de responsabilité. Ainsi les enquêteurs en sources ouvertes devraient-ils, dans la mesure de ce qui est possible et raisonnable, tenir des registres de leurs activités. À chaque étape de l'enquête en sources ouvertes, depuis la recherche des éléments utiles jusqu'au rapport d'enquête, en passant par la collecte et l'analyse de ces éléments, les résultats devraient être consignés de façon constante et claire. Toute personne qui se consacre à la collecte d'informations en ligne et à leur traitement devrait être consciente de la possibilité que ses méthodes soient remises en question devant la justice et qu'elle-même soit amenée à comparaître. La consignation des faits d'enquête peut se faire manuellement ou au moyen des processus automatisés de divers logiciels. Pour autant que la façon de procéder soit constante et consciencieuse, elle peut être manuelle ou automatique. Dans le second cas, elle doit être comprise par les utilisateurs et pouvoir être expliquée devant le tribunal par les utilisateurs ou les concepteurs. L'enquêteur ou l'enquêtrice en sources ouvertes doit consigner tout outil ou logiciel utilisé dans le cadre de ses travaux.

2. Compétence

26. Les enquêteurs en sources ouvertes doivent être adéquatement formés et disposer des compétences techniques voulues pour mener à bien leurs activités. Ils doivent mener leurs travaux en ligne d'une manière professionnelle et conforme à la déontologie, sans s'approprier le travail d'autrui, en mentionnant toutes les parties qui ont contribué à l'enquête (pour autant que cela soit sûr et que ces parties le souhaitent), et en rendant fidèlement compte des données, y compris de toute lacune que pourraient présenter les contenus en ligne. Les enquêteurs et les processus d'enquête en sources ouvertes doivent également, selon qu'il convient, rester flexibles, en phase avec les évolutions, et réceptifs aux nouvelles technologies et techniques. En outre, les organisations et les équipes d'enquête devraient disposer de mécanismes pour veiller à ce que les procédures établies soient suivies en toutes circonstances.

3. Objectivité

27. L'objectivité est un principe fondamental qui régit toutes les enquêtes, qu'elles s'effectuent en ligne ou hors ligne. Les enquêteurs en sources ouvertes devraient avoir à l'esprit que des préjugés personnels, culturels et structurels peuvent affecter leurs activités et que des contre-mesures doivent être prises pour garantir l'objectivité du travail effectué. Ils doivent veiller à entreprendre leurs investigations en toute objectivité, en concevant et en appliquant une pluralité d'hypothèses de travail, sans privilégier telle ou telle théorie pour expliquer les résultats de leurs travaux. Le souci d'objectivité revêt une importance particulière lorsque l'enquête porte sur des sources ouvertes numériques, en raison de la façon dont l'information est structurée en ligne et présentée aux utilisateurs d'Internet. Le navigateur, le moteur de recherche ainsi que les termes et la syntaxe de recherche peuvent conduire à des résultats très différents, même lorsque la requête sous-jacente reste inchangée. Les partis pris inhérents à l'architecture d'Internet et aux algorithmes employés par les moteurs de recherche et les sites Web peuvent

compromettre l'objectivité des résultats d'une recherche[21]. Ces résultats peuvent aussi être influencés par un certain nombre de facteurs techniques, tels que l'appareil utilisé et l'endroit où il se trouve, ainsi que l'historique des recherches de l'utilisateur ou de l'utilisatrice, et ses activités antérieures sur Internet. Les enquêteurs en sources ouvertes devraient pondérer l'influence de tels facteurs en recourant à des moyens technologiques qui permettent d'obtenir des résultats aussi divers que possibles, par exemple, en multipliant les requêtes et en utilisant différents moteurs de recherche et navigateurs[22]. Les enquêteurs devraient avoir conscience d'autres facteurs susceptibles d'influencer les résultats de leurs recherches, notamment des anomalies de l'environnement numérique qui font que des informations en ligne ne soient pas accessibles dans une égale mesure à différents groupes ou différentes franges de la société[23]. Enfin, les enquêteurs devraient toujours s'efforcer de penser et de remédier à leurs propres idées préconçues, qui peuvent être conscientes ou inconscientes[24].

4. Légalité

28. Les enquêtes en sources ouvertes devraient respecter la législation en vigueur, ce qui veut dire que les enquêteurs doivent avoir une compréhension de base des lois qui s'appliquent à leur travail. Ils devraient tout particulièrement être au fait des textes qui protègent les données et du droit à la vie privée, protégé par le droit international des droits humains[25]. Le fait qu'une information soit accessible au public ne signifie pas nécessairement que sa collecte et son utilisation ne concernent pas la vie privée. Les enquêteurs en sources ouvertes doivent considérer l'incidence de leurs actes sur la vie privée, compte tenu notamment du fait qu'une personne peut raisonnablement s'attendre à ce que sa sphère personnelle soit

21 Voir Safiya Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York, New York University Press, 2018) ; Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York, Picador, 2019).

22 Voir, par exemple, Paul Myers, « How to conduct discovery using open source methods », dans *Digital Witness, Using Open Source Information for Human Rights Investigation, Documentation and Accountability*, Sam Dubberley, Alexa Koenig et Daragh Murray, dir. (Oxford, Oxford University Press, 2020) (examine le fait que le choix des moteurs et des termes de recherche peut orienter les résultats des enquêtes en sources ouvertes).

23 Voir, par exemple, Alexa Koenig et Ulic Egan, « Hiding in plain site: using online open source information to investigate sexual violence and gender-based crimes », dans *Technologies of Human Rights Representation*, James Dawes et Alexandra S. Moore, dir. (examine le fait que l'accès relativement limité des femmes aux smartphones et le langage codé utilisé en ligne par les personnes qui ont subi des violences fondées sur le genre peuvent réduire la quantité et la disponibilité d'informations de sources ouvertes concernant ces crimes, et le fait que la prépondérance des hommes dans les emplois liés à la technologie et dans les travaux d'enquête sur les cimes de guerre peut réduire la probabilité que les processus de détection automatisés ou manuels produisent des informations de sources ouvertes sur les crimes de genre). Pour un examen plus approfondi des biais, voir chap. II.C (Principes déontologiques) et V.B (Appréciation du paysage numérique) ci-dessous.

24 Voir, par exemple, Forensic Science Regulator, *Cognitive Bias Effects Relevant to Forensic Science Investigations, FSR-G-217* (Birmingham, Royaume-Uni, 2015) (examine les divers types de biais cognitifs qui peuvent avoir un effet négatif sur la qualité des enquêtes, notamment le biais d'anticipation, le biais de confirmation, l'effet d'ancrage, le biais de contexte, l'effet de rôle et l'effet de reconstitution) ; Wayne A. Wallace, *The Effect of Confirmation Bias on Criminal Investigative Decision Making* (Minneapolis, Walden University ScholarWorks, 2015) (explique le biais de confirmation comme étant le fait pour les enquêteurs de rechercher ou de croire les informations qui confirment la version des faits qu'ils privilégient, et qui les amène à ignorer ou à écarter celles qui vont à l'encontre de cette version) ; Michael Pittaro, « Implicit bias within the criminal justice system », *Psychology Today*, 21 novembre 2018 (examine les biais qui peuvent influencer les enquêtes criminelles de façon générale et propose des techniques de « débiaisement » connues) ; Jon S. Byrd, « Confirmation bias, ethics, and mistakes in forensics », Forensic Pathways, 21 mars 2020 (examine diverses erreurs cognitives et déontologiques qui peuvent déformer l'analyse criminalistique, ainsi que des techniques qui permettent d'éviter ces erreurs). Voir aussi Yvonne McDermott, Daragh Murray et Alexa Koenig, « Digital accountability symposium: whose stories get told, and by whom? Representativeness in open source human rights investigations », Opinio Juris, 19 décembre 2019 (examine le fait que les enquêtes en sources ouvertes peuvent avoir un effet négatif sur les types de violations rapportées et sur la possibilité qui est donnée aux victimes et aux témoins d'être entendus, ainsi que le comment de la construction des récits de violations massives des droits humains) ; projet dirigé par Yvonne McDermott intitulé « The future of human rights investigations: using open source intelligence to transform the documentation and discovery of human rights violations » (L'avenir des enquêtes relatives aux droits de l'homme : l'utilisation du renseignement de sources ouvertes pour transformer la constitution des dossiers sur les violations des droits humains et la découverte de ces violations).

25 L'article 12 de la Déclaration universelle des droits de l'homme dispose que nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation, et que toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. Le Pacte international relatif aux droits civils et politiques dispose de même en son article 17 que nul ne sera sujet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation, et que toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

respectée dans différents espaces numériques. Les enquêteurs devraient aussi être conscients de l'effet mosaïque, c'est-à-dire du fait que des données publiques, même rendues anonymes, peuvent donner lieu à une réidentification lorsque suffisamment d'ensembles de données contenant des informations similaires ou complémentaires sont diffusées ou combinées[26]. En outre, les enquêteurs devraient savoir que, dans certaines juridictions, la surveillance continue et persistante de personnes en ligne, ou la collecte systématique et la conservation à long terme de données personnelles, peut nécessiter des permissions et des garanties supplémentaires, en raison de préoccupations particulières quant à l'incidence de telles activités sur la vie privée[27].

5. Conscience de la sécurité

29. Alors que la prise en compte de la sécurité dès la conception[28] porte sur l'architecture et l'infrastructure de l'enquête et de toute activité collatérale, la conscience de la sécurité est un principe qui vise les considérations que chaque personne doit avoir à l'esprit lorsqu'elle travaille, à commencer par la conscience de son comportement en ligne. Toutes les personnes qui enquêtent en ligne devraient être suffisamment conscientes des questions de sécurité opérationnelle pour réduire au minimum les traces numériques qu'elles laissent, et connaître les risques que peuvent comporter leurs activités. Les organisations qui mènent des enquêtes en sources ouvertes devraient veiller à ce que leurs enquêteurs soient formés en matière de sécurité informatique et en maîtrisent les trois grands piliers : a) la confidentialité (par exemple, veiller à ce que seuls les utilisateurs autorisés puissent accéder aux données) ; b) l'intégrité (veiller à ce que les données ne puissent être manipulées ou autrement altérées par des utilisateurs non autorisés ; c) la disponibilité (veiller à ce que les systèmes et les données soient accessibles aux utilisateurs autorisés lorsqu'ils en ont besoin). La formation devrait aussi porter sur la structure de gouvernance d'Internet. Les menaces et les risques devraient être évalués avant d'entreprendre des activités d'enquête en ligne et cette évaluation devrait être revue et modifiée selon que de besoin. La sécurité est la responsabilité de tous, pas seulement des services d'informatique ou des responsables de la gestion des risques de sécurité.

B. Principes méthodologiques

1. Exactitude

30. Il est impératif, au regard de la méthodologie et de la déontologie, de veiller à l'exactitude des enquêtes, et donc à leur qualité, en ne les fondant que sur des éléments crédibles. Les enquêteurs en sources ouvertes devraient s'attacher à être aussi fidèles à la réalité et aussi précis que possible dans leurs enquêtes et dans la présentation de tout résultat, surtout lorsqu'il s'agit de reconnaître les faiblesses des données sous-jacentes ou du dossier tout entier. Ce souci d'exactitude est souvent servi par l'utilisation et la mise à l'épreuve de multiples hypothèses de travail ou par l'examen par les pairs. Ces deux précautions peuvent contribuer à réduire les risques de biais dans la sélection,

[26] « La notion d'effet mosaïque est dérivée de la théorie de la mosaïque applicable aux activités de renseignement, selon laquelle des éléments d'information disparates, qui ne sont que de peu d'utilité considérés individuellement, acquièrent un sens lorsqu'ils sont combinés avec d'autres types d'informations (Pozen 2005). S'agissant des données publiques, il y a effet mosaïque lorsque des données, même anonymisées, qui peuvent sembler inoffensives lorsqu'elles sont considérées isolément, présentent néanmoins un risque de réidentification lorsque sont diffusés suffisamment d'ensembles de données contenant des informations similaires ou complémentaires ». Voir John Czajka *et al.*, *Minimizing Disclosure Risk in HHS Open Data Initiatives* (Washington, Mathematica Policy Research, 2014), appendice E, p. E-7. Disponible en ligne à l'adresse https://aspe.hhs.gov/system/files/pdf/77196/rpt_Disclosure.pdf. Voir aussi David E. Pozen, « The mosaic theory, national security, and the Freedom of Information Act », *Yale Law Journal*, vol. 115, n° 3 (décembre 2005), p. 628 à 679.

[27] Par exemple, au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, la loi prescrit que « les données personnelles traitées [...] à des fins de police ne doivent pas être conservées plus longtemps que nécessaire pour le motif qui en a requis le traitement » (chap. 2 de la loi de 2018 relative à la protection des données, partie 3, chap. 3, art. 39 1)). En application du règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), les données personnelles ne peuvent être collectées que pour « des finalités déterminées, explicites et légitimes », limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées et ne doivent permettre l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (art. 5 et 6).

[28] Voir par. 33 ci-dessous.

l'interprétation et la présentation des données. Les conclusions de nature analytiques ne devraient pas être exagérées ni surestimées. Le fait de recourir à un langage clair, objectif, ancré dans les faits, en évitant de le rendre émotionnel, est une précaution qui protégera l'objectivité réelle et perçue de l'enquête et de ses résultats.

2. Minimisation des données

31. Le principe de minimisation des données veut que les informations numériques ne soient collectées et traitées que si cela est : a) justifié au regard de finalités énonçables ; b) nécessaire au regard de ces finalités ; et c) proportionné à ces finalités[29]. Dans le contexte des enquêtes en sources ouvertes, le contenu en ligne ne doit être collecté que s'il est utile à une enquête précise. Ce principe est plus favorable à la collecte détaillée et manuelle qu'à la collecte en gros et automatisée, étant à noter toutefois que la seconde pourra se justifier dans certaines situations. L'application de ce principe à la collecte de contenus en ligne servira à éviter de collecter de façon excessive, une précaution importante à plusieurs égards. La collecte excessive, préoccupation d'une importance particulière dans le cas des processus automatisés, peut créer ou aggraver les vulnérabilités en matière de sécurité[30], surtout si les enquêteurs sont amenés à ne pas savoir quels types d'informations sont en leur possession. La collecte excessive peut aussi poser des problèmes du point de vue de la vie privée et de la protection des données, lorsqu'un processus automatisé ne fait pas de distinction entre les types de contenus. Enfin, le fait d'éviter la collecte excessive présente aussi l'avantage pratique de réduire au minimum les frais de stockage et de prévenir les embouteillages en aval, à différents stades du cycle d'enquête, tels que l'examen, l'analyse et, lorsqu'une enquête débouche sur une procédure judiciaire, la communication.

3. Conservation

32. Il est tout aussi important d'éviter la collecte insuffisante d'informations que d'en éviter la collecte excessive. Cette recommandation peut revêtir une importance particulière dans le cas des informations en ligne, dont la durée d'existence et de disponibilité est souvent incertaine. Le principe de conservation est conçu pour éviter la collecte insuffisante et, partant, la perte d'éléments utiles et potentiellement probants. Les plateformes de médias sociaux, par exemple, peuvent supprimer des contenus qui vont à l'encontre de leurs conditions de services, même lorsque ces contenus peuvent s'avérer utiles à des enquêteurs. À moins que l'enquêteur ou l'enquêtrice n'adresse, en temps voulu, une demande de conservation du contenu visé à la plateforme, ou ne trouve un autre moyen de le préserver, l'information qu'il contient peut être perdue à tout jamais. De même que les utilisateurs peuvent décider de supprimer ou de modifier leur propre contenu, auquel cas une information originellement publique deviendrait indisponible. Qui plus est, les informations qui se trouvent sur Internet peuvent aisément être décontextualisées, perdues, effacées ou altérées. Pour que les documents numériques restent accessibles et utilisables aux fins de mécanismes d'attribution des responsabilités, ils doivent être activement et soigneusement conservés, à la fois à court terme et à long terme[31].

4. Sécurité dès la conception

33. Le principe de sécurité dès la conception suppose, dans la mesure du possible, la sécurisation par défaut des informations numériques et des opérations en ligne. Les organisations qui mènent en ligne des enquêtes en sources ouvertes devraient investir dans les moyens techniques et structurels nécessaires pour rendre leurs infrastructures matérielles et logicielles anonymes et non attribuables par défaut lorsque les enquêteurs sont en ligne, et assurer la mise en œuvre de ces moyens. Tous les équipements devraient être pourvus de

[29] Le Protocole tire le principe de minimisation des données du règlement général de l'Union européenne relatif à la protection des données, moyennant l'adaptation de ces dispositions au contexte des enquêtes en sources ouvertes (voir art. 5 du règlement).

[30] Voir chap. IV ci-dessous (Sécurité) pour des exemples de failles de sécurité.

[31] Voir chap. VI.D ci-dessous (Préservation) pour plus de détails.

logiciels actualisés pour les protéger contre les logiciels malveillants, ainsi que les paramètres de confidentialité et de sécurité voulus. Les mesures de sécurité devraient être en place dès avant le commencement des activités d'enquête, et elles devraient continuellement faire l'objet de la surveillance, des mises à jour et des ajustements requis. Les enquêteurs, les équipes d'enquête ou les organisations pourraient prévoir des tests en continu, notamment des tests d'intrusion[32], pour veiller à ce que leurs systèmes de sécurité remplissent leur rôle.

C. Principes déontologiques

1. Dignité

34. Les enquêtes devraient être menées en gardant à l'esprit les problématiques de respect de la dignité qu'elles soulèvent et avec la sensibilité voulue vis-à-vis de ces questions, surtout lorsqu'elles touchent aux intérêts protégés par le droit international des droits humains. Les enquêteurs devraient, par exemple, se conformer aux principes de non-discrimination, dont l'application peut déterminer ce qui va donner lieu à enquête, qui enquêtera ou à qui sera accordé le crédit de l'enquête ; ils devraient aussi incorporer à leurs activités des garanties relatives à la sécurité numérique, physique et psychosociale des témoins, des survivants, des autres enquêteurs, des mis en cause et d'autres parties que les enquêtes pourraient affecter négativement. Le principe de dignité peut également influencer ce qui est rendu public de l'enquête, notamment par écrit ou au moyen de documents visuels. Ainsi peut-il ne pas être nécessaire de montrer toute l'étendue de la souffrance ou de la violence endurées. Ce principe garantit que ce sont les normes relatives aux droits humains qui déterminent les principes déontologiques régissant la conduite des enquêtes en sources ouvertes.

2. Humilité

35. Les enquêteurs en sources ouvertes devraient se montrer humbles en reconnaissant leurs limites et en ayant conscience de ce qu'ils ignorent. La bonne compréhension et la bonne interprétation des informations de sources ouvertes peuvent nécessiter une formation spécialisée et la consultation de spécialistes. Faire preuve d'humilité, c'est aussi assumer la responsabilité des erreurs. Lorsque l'enquêteur ou l'enquêtrice découvre qu'il ou elle a commis une erreur, celle-ci doit être soit corrigée, soit signalée à ceux qui peuvent en réduire au minimum les effets néfastes. Idéalement, il devrait y avoir un mécanisme pour signaler les erreurs et pour publier les corrections, à plus forte raison lorsque les enquêtes sont publiques et largement diffusées.

3. Inclusivité

36. Les enquêteurs en sources ouvertes doivent veiller à incorporer dans les enquêtes de multiples perspectives et vécus. Parmi les facteurs qui peuvent influencer l'inclusivité globale d'une enquête menée en ligne figurent sa portée géographique, les violations des droits humains internationaux ou les crimes internationaux sous enquête, et la conscience de la nature inégale des informations en ligne s'agissant des différentes franges de la société[33]. Les équipes d'enquête devraient, elles aussi, être de composition variée, notamment au regard de l'équilibre des genres. En conjonction avec le principe de dignité, le principe d'inclusivité peut influencer l'enquêteur ou l'enquêtrice dans la sélection et l'utilisation des éléments collectés, ainsi que dans leur présentation à différents publics.

4. Indépendance

37. Les enquêteurs en sources ouvertes devraient se protéger et protéger leurs enquêtes contre les influences indues. Ils devraient déceler et éviter tout conflit d'intérêts réel ou perçu et mettre en place des garanties pour atténuer tout conflit inévitable. La transparence du processus, des méthodes et du financement peuvent également contribuer à la bonne appréciation de l'indépendance d'une enquête et protéger son indépendance réelle ou perçue.

[32] Le test d'intrusion simule une cyberattaque pour vérifier la sécurité du système.

[33] Voir chap. V.B ci-dessous (Appréciation du paysage numérique).

5. Transparence

38. Tandis que le principe de responsabilité requiert de l'enquêteur ou de l'enquêtrice qu'il fasse preuve de transparence dans ses méthodes et leurs résultats, le principe déontologique de transparence porte quant à lui sur la façon dont les enquêteurs en sources ouvertes se comportent en ligne et à l'égard du monde extérieur. Il s'agit de ne pas se présenter sous un jour trompeur[34]. S'il est vrai que l'anonymat et la non-attribution, notamment par le biais d'identités virtuelles[35], peuvent s'avérer importants pour des raisons de sécurité, les enquêteurs devraient être conscients des ramifications négatives que peuvent avoir les fausses déclarations, notamment de l'effet dommageable qu'elles peuvent avoir sur la réputation et la crédibilité d'une enquête, d'une équipe ou d'une organisation, ou sur l'intégrité des informations collectées. Obtenir des informations par des moyens trompeurs peut emporter violation du droit à la vie privée de la personne visée ou entacher l'enquête d'irrégularité, surtout si la fausse déclaration utilisée est illégale sous la ou les juridictions compétentes.

[34] Par exemple, en essayant de se joindre à des groupes fermés ou d'établir des connexions sous de faux prétextes.

[35] Pour un examen de la question des identités virtuelles, voir chap. IV.C ci-dessous (Considérations relatives à l'infrastructure).

III

CADRE JURIDIQUE

SOMMAIRE DU CHAPITRE

- La détermination de la législation applicable est essentielle pour décider des informations à collecter et de la meilleure façon de les collecter. Cette législation variera selon l'identité des enquêteurs et de leurs cibles, l'objet des enquêtes et le ressort dans lequel se situent les enquêteurs, les cibles, les données et les procédures judiciaires.
- La conservation des éléments numériques de sorte à en maintenir l'authenticité et à en documenter la chaîne de contrôle augmentera la probabilité que ces éléments puissent être reçus en preuve devant les tribunaux.
- La définition du type d'enquête et de sa finalité (procédure pénale, procédure civile, processus de justice transitionnelle, etc.) déterminera le seuil de preuve à appliquer.
- La violation du droit d'une personne à la vie privée peut entraîner l'exclusion d'éléments de preuve.

39. Les enquêteurs en sources ouvertes doivent avoir une bonne compréhension des cadres juridiques dans lesquels ils mènent leurs activités. Cela comprend la connaissance des corpus juridiques applicables à leurs enquêtes et des cadres juridiques des ressorts dans lesquels ils les mènent. La connaissance des règles de droit matériel applicables aux enquêtes, y compris les éléments constitutifs de violations[36] ou de crimes éventuels, et les formes de participation engageant la responsabilité[37], peut contribuer à mieux cibler les enquêtes tout en augmentant la probabilité que les informations collectées et toute conclusion analytique dégagée puissent servir la justice et l'attribution des responsabilités. De même, la connaissance du droit procédural et des règles de preuve dans les ressorts compétents permet aux enquêteurs d'accomplir un travail qui réponde aux conditions d'utilisation des informations de sources ouvertes dans les procédures judiciaires.

40. Dans le cas des enquêtes touchant au droit pénal international, le cadre juridique sera prescrit par le statut du tribunal, de la cour ou du système judiciaire compétents[38]. Pour les enquêtes mandatées au niveau international, comme dans le cas des commissions d'enquête, le mécanisme qui établit l'enquête prescrira, entre autres paramètres, les corpus juridiques applicables, ainsi que la portée géographique et temporelle de l'enquête[39]. En ce qui concerne les autres enquêtes, dont celles entreprises par les ONG, l'entité responsable peut définir son propre cadre juridique[40].

41. Le présent chapitre a été conçu pour aider les enquêteurs en sources ouvertes à se faire une meilleure idée et à acquérir une meilleure compréhension des finalités possibles de leur travail et à adapter leurs techniques d'enquête en conséquence. Dès lors que les lois applicables varient selon les juridictions, les types d'enquêtes et l'autorité légale de l'entité responsable de l'enquête, les sections suivantes proposent un survol des principales considérations qui interviennent lorsqu'il est enquêté sur des violations possibles du droit international. Il est recommandé que les enquêteurs prennent conseil auprès de juristes qui soient au fait des ressorts et des matières concernés.

---

36 Ainsi l'enquêteur ou l'enquêtrice qui s'intéressent au discours de haine et à l'incitation à la violence devraient-ils comprendre le type de comportement qui atteint le seuil très élevé fixé par l'article 20 2) du Pacte international relatif aux droits civils et politiques. Voir Plan d'action de Rabat sur l'interdiction de l'appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence (A/HRC/22/17/Add.4, appendice), par. 11 et 29, et sa grille d'évaluation du seuil, fondée sur les droits humains, et publiée en 32 langues. Disponible à l'adresse https://www.ohchr.org/fr/freedom-of-expression. En ce qui concerne le discours de haine, voir Stratégie et plan d'action des Nations Unies pour la lutte contre les discours de haine (2019). Disponible à l'adresse www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action_plan_on_hate_speech_FR.pdf.

37 En droit pénal, les auteurs peuvent voir leur responsabilité engagée pour un certain nombre de formes de participation, comme énoncé dans le statut pertinent. Ces modes de responsabilité comprennent la commission directe et indirecte, la commission en tant que coauteur, l'aide et l'encouragement et la responsabilité du supérieur hiérarchique. Voir Jérôme de Hemptinne, Robert Rothet Elies van Sliedregt, dir., *Modes of Liability in International Criminal Law* (Cambridge, Royaume-Uni, Cambridge University Press, 2019).

38 Voir, par exemple, Cour pénale internationale, Règlement de procédure et de preuve (2013) ; Tribunal pénal international pour l'ex-Yougoslavie, Règlement de procédure et de preuve (8 juillet 2015) ; Tribunal pénal international pour le Rwanda, Règlement de procédure et de preuve (13 mai 2015) ; Tribunal spécial résiduel pour la Sierra Leone, Rules of Procedure and Evidence (30 novembre 2018) ; Tribunal spécial pour le Liban, Règlement de procédure et de preuve (10 avril 2019) ; Chambres extraordinaires au sein des tribunaux cambodgiens, Règlement intérieur (3 août 2011).

39 Par exemple, la mission internationale indépendante d'établissement des faits sur la République bolivarienne du Venezuela qui a été créée en septembre 2019 avec pour mandat d'enquêter sur les cas d'exécution extrajudiciaire, de disparition forcée, de détention arbitraire et de torture et autres peines ou traitements cruels, inhumains ou dégradants survenus depuis 2014, et de présenter un rapport sur les résultats de travaux au Conseil des droits de l'homme (résolution 42/25 du Conseil des droits de l'homme, par. 24) ; la Commission d'enquête internationale indépendante sur la République arabe syrienne qui a été créée en 2011 avec pour mandat d'enquêter sur toutes les violations alléguées du droit international des droits de l'homme commises en République arabe syrienne depuis mars 2011, d'établir les faits et circonstances qui pourraient constituer de telles violations et des crimes perpétrés et, si possible, d'en identifier les responsables (résolution S-17/2 du Conseil des droits de l'homme, par. 13) ; l'équipe d'experts internationaux qui a été dépêchée dans les régions du Kasaï de la République démocratique du Congo en 2017 avec pour mandat de réunir et de conserver des informations concernant des violations présumées des droits de l'homme et des violations du droit international humanitaire dans les régions du Kasaï, et de communiquer aux autorités judiciaires de la République démocratique du Congo les conclusions de cette enquête (résolution 35/33 du Conseil des droits de l'homme, par. 10).

40 Il n'est pas rare que des organisations, notamment des ONG, aient leurs propres méthodes internes qui font qu'elles se concentrent sur tel ou tel domaine du droit, comme la torture ou la violence sexuelle et fondée sur le genre, ce qui les guidera aussi pour centrer leurs enquêtes.

A. Droit international public

42. Le Protocole porte sur trois catégories du droit international public qui se chevauchent de façon non négligeable : le droit international humanitaire, le droit international des droits humains et le droit pénal international. Ces catégories se renforcent mutuellement. De fait, l'applicabilité du droit international humanitaire ou du droit pénal international, ou de l'un et l'autre à la fois, ne dispense pas les États de s'acquitter de leurs obligations au regard du droit international des droits humains. Ce qui suit est une vue d'ensemble de chaque domaine de pratique. Elle présente notamment les sources de droit et les caractéristiques distinctives, pour que les enquêteurs en sources ouvertes sachent quelles références devraient guider leurs travaux.

1. Droit international humanitaire

43. Le droit international humanitaire ou « droit des conflits armés » régit la conduite des hostilités et résout les questions humanitaires qui surviennent dans le cadre de tels conflits, lesquels peuvent être de nature internationale ou non internationale[41]. Le droit international humanitaire intervient à partir du moment où un conflit armé se déclenche et jusqu'au moment où la paix est rétablie, bien que ces délimitations ne soient pas toujours certaines ni simples[42]. Les principales sources du droit international humanitaire sont les Conventions de La Haye de 1899 et 1907[43], les Conventions de Genève du 12 août 1949[44] et leurs Protocoles additionnels de 1977[45], ainsi que plusieurs traités régissant l'utilisation de certains types d'armes[46]. Le droit coutumier est également une source importante de droit international humanitaire, en ce qu'il comble des lacunes laissées par les traités. Le droit international coutumier est contraignant pour toutes les parties à un conflit et revêt une pertinence particulière pour les conflits armés non internationaux, en ce que les règles qui en résultent sont plus détaillées que celles du droit international humanitaire de fondement

41 Les conflits armés seront qualifiés d'internationaux ou de non internationaux selon deux critères : la structure des parties aux hostilités et leur statut. Lorsqu'ils sont internationaux, les conflits armés opposent des États souverains, lorsqu'ils sont non internationaux, ils opposent des États et des groupes organisés. Voir Andrew Clapham, Paola Gaeta et Marco Sassòli, dir., *The 1949 Geneva Conventions, A Commentary* (Oxford, Oxford University Press, 2015), chap. 1 et 19.

42 Alors que le début d'un conflit armé international est relativement facile à déterminer puisqu'il résulte de tout usage de la force entre deux États, le début d'un conflit non international se détermine moins simplement. Les conflits armés non internationaux n'existent que si les groupes armés sont suffisamment organisés et si la violence atteint un certain niveau d'intensité, deux facteurs qui appellent une analyse détaillée des faits au cas par cas. Voir Sylvain Vité, « Typologie des conflits armés en droit international humanitaire : concepts juridiques et réalités », *Revue internationale de la Croix-Rouge*, vol. 91, n° 873 (mars 2009), p. 3 ainsi que 6 et 7 de l'article. Il y a également désaccord quant au moment où un conflit armé prend fin et où la paix est réalisée. Les cessez-le-feu et les accords de paix sont certes indicatifs de la fin d'un conflit armé, mais ils ne sont pas déterminants à cet égard. Divers critères ont été proposés pour déterminer la fin d'un conflit armé, à savoir l'arrêt général des opérations militaires une fois conclu un accord général de paix, l'existence d'un règlement pacifique et la cessation des critères définissant l'existence d'un conflit. Voir Nathalie Weizmann, « The end of armed conflict, the end of participation in armed conflict, and the end of hostilities: implications for the detention operations under the 2001 AUMF », *Columbia Human Rights Law Review*, vol. 47, n° 3 (2016), p. 221 à 224.

43 Respectivement, la Convention concernant les lois et coutumes de la guerre sur terre (deuxième Convention de La Haye) et la Convention concernant les lois et coutumes de la guerre sur terre (quatrième Convention de La Haye).

44 Voir Convention de Genève pour l'amélioration du sort des blessés et des malades dans les forces armées en campagne (première Convention de Genève) ; Convention de Genève pour l'amélioration du sort des blessés, des malades et des naufragés des forces armées sur mer (deuxième Convention de Genève) ; Convention de Genève relative au traitement des prisonniers de guerre (troisième Convention de Genève) ; Convention de Genève relative à la protection des personnes civiles en temps de guerre (quatrième Convention de Genève).

45 Voir Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I) ; Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés non internationaux (Protocole II).

46 Voir, par exemple, Convention sur l'interdiction de la mise au point, de la fabrication et du stockage des armes bactériologiques (biologiques) ou à toxines et sur leur destruction ; Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination ; Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction ; Convention sur l'interdiction de l'emploi, du stockage, de la production et du transfert des mines antipersonnel et sur leur destruction ; Convention sur les armes à sous-munitions. Voir aussi Comité international de la Croix-Rouge (CICR), « Armes », 20 octobre 2010. Disponible à l'adresse www.icrc.org/fr/document/armes.

conventionnel[47]. Jusqu'au début des années 1990, les principaux mécanismes d'application effective du droit international humanitaire avaient été les tribunaux militaires nationaux, devant lesquels les États demandaient des comptes à leur propre personnel de troupe et à leurs propres officiers. Avec l'avènement des tribunaux pénaux internationaux, certaines violations graves du droit international humanitaire ont été codifiées dans les statuts fondateurs de ces juridictions en tant que crimes de guerre[48], ouvrant ainsi la voie à l'application effective du droit international humanitaire au niveau international. Certains États ont également codifié des crimes de guerre dans leur législation domestique[49], ce qui permettait de les poursuivre devant leur système judiciaire ordinaire plutôt que devant des instances militaires. Des affaires nationales peuvent être poursuivies dans le pays du conflit ou, de plus en plus souvent, dans d'autres pays, en vertu du principe de compétence universelle[50]. Plusieurs États ont mis sur pied des services nationaux chargés de la répression des crimes de guerre afin de poursuivre de tels actes. Les tribunaux pénaux internationaux et les tribunaux nationaux apportent leur contribution au corpus jurisprudentiel croissant en matière de droit international humanitaire, lui-même source de droit importante dont les règles peuvent être contraignantes dans certaines juridictions.

2. Droit international des droits humains

44. Le droit international fait obligation aux États de respecter, protéger et réaliser les droits humains. La Déclaration universelle des droits de l'homme, adoptée en 1948, pose les fondements du droit international des droits humains. Bien que celui-ci relève de l'aspiration, sans être légalement contraignant, certaines de ses dispositions font partie du droit international coutumier[51]. Il a aussi inspiré deux pactes et un riche ensemble de traités relatifs aux droits humains[52]. Les États ne sont liés que par les pactes et les traités qu'ils ont signés et ratifiés, à moins que les règles contenues dans ces conventions n'atteignent le statut de règles de droit international

47 Voir CICR, « Le droit international humanitaire coutumier », 29 octobre 2010. Disponible à l'adresse www.icrc.org/fr/document/DIH-coutumier. Voir aussi CICR, « Bienvenue dans la base de données sur le DIH coutumier ». Disponible à l'adresse https://ihl-databases.icrc.org/customary-ihl/fre/docs/home.

48 Par exemple, l'article 8 du Statut de Rome de la Cour pénale internationale codifie le droit international humanitaire dans sa définition des crimes de guerre.

49 Voir, par exemple : Afrique du Sud (loi de 2012 relative à l'application des Conventions de Genève) ; Australie (loi de 1945 relative aux crimes de guerre, telle que modifiée, art. 7) ; Bosnie-Herzégovine (Code pénal, art. 171 à 184) ; Kenya (loi de 2008 relative aux crimes internationaux, art. 6 1) c) et 6 2) à 4)) ; Nouvelle-Zélande (loi de 2000 relative aux crimes internationaux et à la Cour pénale internationale, art. 11).

50 En vertu de la « compétence universelle », une juridiction interne est habilitée à poursuivre des individus pour des crimes graves commis en violation du droit international (tels que les crimes contre l'humanité, les crimes de guerre, le génocide et la torture) hors les frontières de l'État concerné, le principe étant que de tels crimes portent préjudice à la communauté et à l'ordre internationaux, et qu'un État peut agir pour protéger lesdits intérêts. Voir International Justice Resource Center, « Universal jurisdiction ». Disponible à l'adresse https://ijrcenter.org/cases-before-national-courts/domestic-exercise-of-universal-jurisdiction.

51 De nombreux pays, responsables de l'ONU et spécialistes ont déclaré que la majorité, voire la totalité, des articles de la Déclaration universelle des droits de l'homme relevaient du droit international coutumier. Plus spécifiquement, les interdictions qui frappent l'esclavage, la privation arbitraire de la vie, la torture, la détention arbitraire et la discrimination raciale, telles que les codifie la Déclaration universelle des droits de l'homme, sont acceptées comme relevant du droit international coutumier. Voir Hurst Hannum, « The status of the Universal Declaration of Human Rights in national and international law », *Georgia Journal of International and Comparative Law*, vol. 25, n° 1 (1996), p. 322 à 332 et 341 à 346.

52 Voir Convention internationale sur l'élimination de toutes les formes de discrimination raciale ; Pacte international relatif aux droits civils et politiques ; Pacte international relatif aux droits économiques, sociaux et culturels ; Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes ; Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants ; Convention relative aux droits de l'enfant. Pour plus d'informations sur les principaux instruments des Nations Unies relatifs aux droits de l'homme, voir HCDH, « The core international human rights instruments and their monitoring ». Disponible à l'adresse www.ohchr.org/EN/ProfessionalInterest/Pages/CoreInstruments.aspx.

coutumier[53]. Le droit international des droits humains a également été incorporé dans le cadre statutaire de nombreux tribunaux pénaux internationaux. À cela s'ajoute que plusieurs juridictions régionales des droits de l'homme ont été créées par des conventions internationales pour statuer sur les actions intentées contre des parties à ces conventions pour violation du droit international des droits de l'homme. Il en est ainsi de la Cour africaine des droits de l'homme et des peuples[54], de la Cour européenne des droits de l'homme[55] et de la Cour interaméricaine des droits de l'homme[56]. Il existe, au niveau régional, des organes supplémentaires des droits de l'homme. Ceux-ci comprennent la Commission africaine des droits de l'homme et des peuples, le Comité européen des droits sociaux et la Commission interaméricaine des droits de l'homme, qui tous continuent d'alimenter la jurisprudence relative au droit international des droits de l'homme.

45. Les organisations internationales jouent également un rôle clef dans le développement et la normalisation du droit international coutumier des droits humains[57]. Les rapports thématiques que le HCDH et d'autres entités internationales publient sur certains aspects du droit contribuent à l'établissement de normes et au développement du droit souple. Les organes conventionnels[58] produisent des rapports[59], des recueils de jurisprudence[60] et d'autres formes d'orientation, notamment des observations générales et des recommandations[61] qui contribuent au développement et à la compréhension des articles de leurs traités respectifs. De même, les procédures spéciales du Conseil des droits de l'homme jouent un rôle dans l'évolution des aspects normatifs du droit international des droits humains[62], comme le font d'autres mécanismes, telles les missions d'établissement des faits et les commissions d'enquête.

53 Le droit international coutumier s'entend des obligations internationales qui résultent de pratiques internationales établies, à la différence des obligations découlant des conventions et traités écrits. Il procède de la pratique générale et constante que les États observent parce qu'ils s'y sentent juridiquement obligés. Une composante fondamentale du droit international coutumier est le *jus cogens*, constitué de certains principes fondamentaux et supérieurs du droit international. Voir, par exemple, Legal Information Institute, « Customary international law » et « *Jus cogens* », Cornell Law School. Disponible à l'adresse www.law.cornell.edu/wex.

54 Créée en application de la Charte africaine des droits de l'homme et des personnes (Charte de Banjul).

55 Créée en application de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (Convention européenne des droits de l'homme).

56 Créée en application de la Convention américaine relative aux droits de l'homme (Pacte de San José).

57 Les organisations internationales comprennent notamment la Cour pénale internationale, l'Organisation internationale pour les migrations et l'Organisation pour l'interdiction des armes chimiques, ainsi que des mécanismes relatifs aux droits humains, tels que les procédures spéciales et les commissions d'enquête du Conseil des droits de l'homme ou leurs équivalents. Les procédures spéciales exécutent leurs mandats vis-à-vis de tous les États Membres de l'ONU ; ils ne dépendent pas de la ratification d'un traité donné. Il y a des différences entre les règles juridiques et les rouages de ces mécanismes de protection des droits humains, de même qu'entre les méthodes et normes de collecte des informations. Par exemple, le principal mode de fonctionnement du Groupe de travail sur la détention arbitraire consiste à recevoir des communications concernant des cas individuels de la part des personnes concernées, de leurs familles ou de leurs représentants, ainsi que de gouvernements, d'ONG et d'organismes nationaux. Le Groupe de travail enquête alors sur les cas rapportés dans les communications, y compris au moyen de visites de pays. Voir A/HRC/36/38 pour les méthodes de travail les plus récentes du Groupe de travail. Les commissions d'enquête, quant à elles, sont créées par le Conseil des droits de l'homme au cas par cas, et mènent habituellement leurs propres enquêtes selon les termes de leurs mandats, souvent au moyen de visites de pays au cours desquelles, entre autres activités, elles s'entretiennent avec des témoins. Voir, par exemple, les termes de référence de la Commission d'enquête sur le Burundi. Disponibles à l'adresse www.ohchr.org/Documents/HRBodies/HRCouncil/CoIBurundi/TermesderéférenceCOIBurundi.pdf.

58 Voir, par exemple, HCDH, « Organes conventionnels ». Disponible à l'adresse www.ohchr.org/fr/treaty-bodies.

59 Les rapports peuvent se présenter sous la forme d'observations finales dans lesquelles l'organe conventionnel examine le rapport soumis par un État partie et d'autres parties prenantes concernant le respect par l'État en question de ses obligations au titre d'un traité donné. Certains organes conventionnels ont également la possibilité d'établir des rapports d'enquête. Voir, par exemple, Comité pour l'élimination de la discrimination à l'égard des femmes, « Procédure d'enquête ». Disponible en anglais à l'adresse www.ohchr.org/fr/treaty-bodies/cedaw/inquiry-procedure.

60 Les organes conventionnels rendent des constatations sur des cas particuliers à la suite de communications émanant de particuliers. Voir, à titre général, HCDH, « Organes conventionnels – Plaintes concernant des violations des droits de l'homme – Communications émanant de particuliers ». Disponible à l'adresse www.ohchr.org/fr/treaty-bodies/human-rights-bodies-complaints-procedures.

61 Voir HCDH, « Organes Conventionnels – Observations générales ». Disponible à l'adresse www.ohchr.org/fr/treaty-bodies/human-rights-treaty-bodies-general-comments.

62 Voir, à titre général, HCDH, « Procédures spéciales du Conseil des droits de l'homme ». Disponible à l'adresse www.ohchr.org/fr/special-procedures-human-rights-council.

46. Comme le droit international humanitaire, le droit international des droits humains est présent dans le cadre législatif de nombreux pays, soit par l'effet de traditions juridiques monistes qui appliquent directement les obligations internationales dans la sphère nationale, soit par l'incorporation directe du droit international dans la législation interne, soit encore par le jeu de la compétence universelle, ce qui crée une abondante jurisprudence relative à ce droit[63].

3. Droit pénal international

47. Le droit pénal international s'applique tant en temps de paix qu'en temps de conflit armé, engageant la responsabilité pénale des individus qui commettent des crimes de droit international, notamment des crimes de guerre, des crimes contre l'humanité et des crimes de génocide[64]. Ces infractions, parfois collectivement qualifiées d'« atrocités criminelles », de « crimes atroces »[65] ou de « crimes internationaux graves », ont été dans une large mesure codifiées dans le Statut de Rome, généralement considéré comme représentatif du droit pénal international coutumier. Le droit pénal international réprime aussi des crimes qui ne sont pas codifiés dans le Statut de Rome, comme le terrorisme[66]. Il peut y avoir un certain chevauchement entre le droit pénal international et le domaine apparenté du droit pénal transnational, qui criminalise des actes transfrontaliers comme la traite des personnes et le trafic des drogues, des armes et d'autres biens illicites[67]. À la différence du droit international humanitaire et du droit international des droits humains qui visent la responsabilité des États, le droit pénal international concerne la responsabilité pénale individuelle. Les affaires relevant du droit pénal international peuvent être jugées devant des juridictions pénales internes, des juridictions pénales hybrides[68], des juridictions pénales internationales[69], dont la Cour pénale internationale, ou des juridictions internes exerçant la compétence universelle. Les sources du droit pénal international comprennent les textes constitutifs des cours et tribunaux (par exemple, les résolutions du Conseil de sécurité et les statuts, règlements de procédure et de preuve et autres règles des juridictions) et la législation interne des États qui exercent une compétence sur des crimes internationaux. Une autre source du droit pénal international est la jurisprudence, qui peut être contraignante ou persuasive selon le ressort[70].

B. Compétence et responsabilité

48. La compétence est un terme juridique qui renvoie à l'autorité qui est reconnue à une entité judiciaire, telle qu'une cour ou un tribunal, de dire le droit, de statuer sur son fondement et d'en assurer l'application. Aux fins du Protocole, la justice et l'attribution des responsabilités s'entendent au sens large de différents types de processus judiciaires et non judiciaires. La responsabilité attribuée pour les crimes internationaux, pour les violations du droit international des droits humains ou les violations du droit international humanitaire peut résulter d'une procédure

63 Amnesty International, *Universal Jurisdiction: A Preliminary Survey of Legislation Around the World – 2012 Update* (Londres, 2012), p. 1 et 2.

64 Robert Cryer, Darryl Robinson et Sergey Vasiliev, *An Introduction to International Criminal Law and Procedure*, 4e éd. (Cambridge (Royaume-Uni), Cambridge University Press, 2019), chap. 15.

65 Le « nettoyage ethnique », bien qu'il ne figure pas dans le Statut de Rome et qu'il n'ait pas été qualifié de crime à part entière en droit international, est considéré comme relevant de la catégorie des « atrocités criminelles ». À cet égard, veuillez vous référer à ONU, *Cadre d'analyse des atrocités criminelles : Outil de prévention*, p. 1. Disponible à l'adresse www.un.org/en/genocideprevention/documents/publications-and-resources/Framework of Analysis for Atrocity Crimes_FR.pdf.

66 Voir résolution 1757 (2007) du Conseil de sécurité, annexe, pièce jointe (Statut du Tribunal spécial pour le Liban), art. 2.

67 Cryer, Robinson et Vasiliev, *An Introduction to International Criminal Law and Procedure*, chap. 15.

68 Cette expression désigne, entre autres, les Chambres extraordinaires au sein des tribunaux cambodgiens, le Tribunal spécial pour la Sierra Leone, le Tribunal spécial pour le Liban, les Chambres spécialisées pour le Kosovo et le Bureau du Procureur spécialisé, et la Cour pénale spéciale en République centrafricaine.

69 Cette expression désigne la Cour pénale internationale (juridiction permanente) et le Tribunal pénal international pour l'ex-Yougoslavie, le Tribunal pénal international pour le Rwanda et le Mécanisme international appelé à exercer les fonctions résiduelles des Tribunaux pénaux (juridictions spéciales).

70 Voir Rosa Theofanis, « The doctrine of res judicata in international criminal law », *International Criminal Law Review*, vol. 3, no 3 (2003).

judiciaire, laquelle peut être pénale, civile ou administrative, ou de processus qui ne sont pas juridiquement contraignants, comme les rapports des enquêtes internationales relatives aux droits humains, dans le cas des commissions d'enquête et des missions d'établissement des faits notamment, ou d'autres mécanismes de justice transitionnelle, tels que ceux consacrés à la recherche de la vérité. Les enquêteurs devraient s'efforcer, dans la mesure du possible, de considérer l'éventail des ressorts dans lesquels les responsabilités pourraient être établies.

49. L'enquêteur ou l'enquêtrice en sources ouvertes devrait relever les mécanismes d'attribution des responsabilités qui pourraient avoir un rapport avec ses travaux, ainsi que les cadres dans lesquels les éléments collectés peuvent ou pourraient être reçus aux fins de l'établissement des faits. Toutefois, aux premiers stades des enquêtes internationales, ces possibilités peuvent ne pas être connues ou claires. Ce sera particulièrement vrai lorsque l'État sur le territoire duquel les infractions ont été commises n'a pas de système judiciaire en état de fonctionner, ou lorsque la communauté internationale n'est pas encore suffisamment saisie de la question pour la soumettre à enquête. En outre, il peut ne pas être possible de prédire tous les ressorts qui pourraient être saisis à l'avenir. Lorsque les enquêteurs en sources ouvertes ne sont pas au fait du mécanisme ou de la juridiction compétente, il devraient s'employer à collecter et à conserver les informations de sorte à en maximiser l'utilité pour le plus large éventail d'instances potentiellement compétentes. S'ils connaissent les exigences de l'instance qui se prononcera sur l'affaire, ils devraient adapter leurs processus à ces conditions particulières.

50. La compétence peut s'établir comme suit :

a) La compétence territoriale est le pouvoir de la juridiction de connaître d'affaires portant sur des actes qui seraient survenus dans un territoire défini. La compétence des tribunaux internationaux est habituellement limitée aux territoires des États qui en ont ratifié le traité fondateur ;

b) La compétence temporelle est le pouvoir de la juridiction de connaître d'affaires portant sur des actes qui seraient survenus pendant une période prescrite ;

c) La compétence personnelle est le pouvoir de la juridiction de rendre des décisions concernant une partie à la procédure ;

d) La compétence matérielle est le pouvoir d'une juridiction de connaître d'affaires d'un type particulier ou d'affaires se rapportant à une matière particulière ;

e) La compétence universelle est le pouvoir qu'une juridiction s'accorde de juger une personne accusée sans égard au lieu où aurait été commis le crime présumé, ni à la nationalité ou au pays de résidence du justiciable, ou à tout autre rapport avec l'entité chargée des poursuites.

C. Pouvoirs et devoirs d'enquête

51. Les pouvoirs d'enquête sont ceux qui, officiellement octroyés en vertu de la loi, habilitent une entité à enquêter dans un ressort donné. De façon assez similaire aux limites imposées à la compétence judiciaire, une entité relevant de la magistrature assise ou debout ne peut mener d'enquêtes que dans les limites prévues par la loi[71]. Les pouvoirs d'enquête peuvent s'étendre à ceux de contraindre un témoin à déposer, de saisir des documents et d'exécuter des mandats de perquisition. L'entité chargée d'enquêter peut être tenue par la loi de suivre certaines procédures strictes ou, dans certains cas, être habilitée à élaborer elle-même ses procédures[72].

52. La plupart des autres entités chargées d'enquêter sur des violations du droit international n'ont généralement pas été investies de pouvoirs d'enquête ou de moyens contraignants pour collecter des éléments de preuve, comme la saisie ou le mandat

[71] Voir Justia, « Agency investigations ». Disponible à l'adresse https://www.justia.com/administrative-law/agency-investigations/.

[72] Id.

d'arrêt. Elles peuvent par conséquent dépendre entièrement des informations de sources ouvertes et d'informations volontairement fournies prenant la forme de documents, de fichiers numériques et de témoignages.

53. Généralement, les pouvoirs d'enquête sont assortis de devoirs définis[73]. Bien que certains enquêteurs ne soient pas investis de pouvoirs de police ou d'autres prérogatives légales, il est recommandé, dans la mesure du possible, que tous les enquêteurs s'efforcent de se plier aux devoirs essentiels de leurs collègues mandatés par la loi, afin d'assurer la qualité des enquêtes. Parmi les devoirs et les obligations des enquêteurs mandatés par la loi, ainsi que des procureurs, figurent le devoir d'enquêter à la fois sur les éléments à charge et à décharge, le devoir de protéger les témoins, le devoir de conserver la preuve, le devoir de veiller à l'équité de la procédure, et l'obligation de respecter les droits des personnes accusées.

54. Dans les procès pénaux, les procureurs sont également tenus de communiquer à la défense les informations et les éléments de preuve pertinents qui sont en leur possession[74]. Il ne s'agit pas seulement de la preuve produite au procès, mais de toute information à charge comme à décharge recueillie dans le cadre de l'enquête, y compris en ce qui concerne la crédibilité des témoins[75]. Il y a certaines exceptions s'agissant d'informations privilégiées ou susceptibles de mettre une personne en danger. Un tribunal peut ordonner la non-communication de l'identité d'une victime ou d'un témoin qui pourraient être mis en danger par telle communication, mais cette mesure n'est jamais garantie[76]. De nombreuses juridictions pénales ont des règles de communication qui obligent le parquet à révéler tout élément tendant à disculper la personne mise en cause[77]. L'enquêteur ou l'enquêtrice en sources ouvertes chargés d'un dossier qui a la moindre chance de faire l'objet d'une procédure judiciaire devraient tenir compte de ces obligations lorsqu'ils effectuent leurs travaux[78]. Il est plusieurs autres raisons pour lesquelles les enquêteurs devraient garder à l'esprit la possibilité qu'une information doive être communiquée. Par exemple, si les procureurs sont tenus d'examiner tous les éléments recueillis dans le cadre d'une enquête, les enquêteurs devraient se garder de collecter en masse, car les gros volumes d'informations peuvent s'avérer difficiles, voire impossibles à examiner. Cela vaut aussi pour la conservation

[73] Par exemple, l'article 54 du Statut de Rome définit les devoirs et les pouvoirs du Procureur en matière d'enquêtes, habilitant celui-ci notamment à enquêter, à recueillir et à examiner des éléments de preuve, à interroger les victimes et les témoins, et à rechercher la coopération des États et des organisations internationales.

[74] Voir, par exemple, Tribunal pénal international pour l'ex-Yougoslavie, Règlement de procédure et de preuve, art. 66 A) ; Tribunal pénal international pour le Rwanda, Règlement de procédure et de preuve, art. 66 A) ; Tribunal spécial pour le Liban, *Rules of Procedure and Evidence*, art. 110 A).

[75] Voir, par exemple, Cour pénale internationale, Règlement de procédure et de preuve, règles 76 à 84 ; Tribunal pénal international pour l'ex-Yougoslavie, Règlement de procédure et de preuve, art. 66 A) ii) ; Tribunal pénal international pour le Rwanda, Règlement de procédure et de preuve, art.66 A) ii) ; Tribunal spécial pour la Sierra Leone, *Rules of Procedure and Evidence*, art. 66 A) ii) ; Tribunal spécial pour le Liban, Règlement de procédure et de preuve, art. 110 A) ii) ; Chambres spéciales chargées de connaître des crimes graves au Timor oriental, *Transitional Rules of Criminal Procedure*, art. 24.4.

[76] Voir, par exemple, Cour pénale internationale, Règlement de procédure et de preuve, règle 81 4) ; Tribunal pénal international pour l'ex-Yougoslavie, Règlement de procédure et de preuve, art. 69 ; Tribunal pénal international pour le Rwanda, Règlement de procédure et de preuve, art. 69 ; Tribunal spécial pour la Sierra Leone, Rules of Procedure and Evidence, art. 69 ; Tribunal spécial pour le Liban, Règlement de procédure et de preuve, art. 115et 116 ; Chambres spéciales chargées de connaître des crimes graves au Timor oriental, *Transitional Rules of Criminal Procedure*, art. 24.6.

[77] Voir, par exemple, Tribunal pénal international pour l'ex-Yougoslavie, Règlement de procédure et de preuve, art. 68 ; Tribunal pénal international pour le Rwanda, Règlement de procédure et de preuve, art. 68 ; Tribunal spécial pour la Sierra Leone, *Rules of Procedure and Evidence*, art. 68 ; Tribunal spécial pour le Liban, Règlement de procédure et de preuve, art. 113 ; Statut de Rome de la Cour pénale internationale, art. 67 2) ; Chambres spéciales chargées de connaître des crimes graves au Timor oriental, Rules of Procedure and Evidence, art. 24.4 c). Un élément de preuve à décharge est un élément de preuve qui tend à disculper une personne mise en cause. Aux États-Unis, la doctrine Brady, règle de communication préalable au procès pénal établie par la Cour suprême, oblige le parquet à communiquer tout élément de preuve à décharge à la défenderesse ou au défendeur. Voir Brady v. Maryland, 378 U.S. 83 (1963).

[78] Comme il se peut qu'en exécution des obligations de communication une partie ou la totalité des éléments collectés doivent être fournis à la défense, les enquêteurs en sources ouvertes peuvent se trouver dans l'impossibilité de protéger certaines identités ou autres informations sensibles.

et le stockage des informations collectées, y compris leur marquage, ce qui sera d'une grande utilité pour ceux qui chercheront à extraire et à examiner les éléments par la suite.

D. Règlements de procédure et de preuve

55. Dans le cadre d'une enquête à des fins judiciaires, la tâche principale des enquêteurs en sources ouvertes est de collecter des informations pertinentes et authentiques susceptibles de fonder des constatations de fait et des conclusions de droit. Dans le cas des juridictions internationales en particulier, il faut veiller à ce que tout élément de source ouverte recueilli soit admissible ainsi que pertinent, fiable et probant. Les enquêtes criminelles se distinguent des autres par le niveau de preuve plus élevé[79] et les règles de procédure et de preuve plus exigeantes auxquelles elles sont astreintes, notamment pour ce qui est de la recevabilité, afin de respecter la régularité de la procédure et le droit de toute personne accusée à un procès équitable[80]. Bien que le seuil de recevabilité de la preuve soit généralement placé plus bas devant les juridictions internationales que devant certaines juridictions nationales, les méthodes de collecte des éléments de preuve affecteront toutefois le poids que leur reconnaîtront les juges statuant sur les affaires internationales. Il en est ainsi devant toutes les juridictions. À une époque marquée par la prolifération de l'information numérique, avec ce que cela comporte aussi de mésinformation et de désinformation[81], il est crucial que les enquêteurs soient en mesure de déterminer si les informations de sources ouvertes sont authentiques, et d'établir ou de réfuter leur véracité avec suffisamment de précision[82].

56. Aux fins des procédures judiciaires, la recevabilité renvoie à la question de savoir si un élément présenté par une partie à la procédure peut être versé au dossier de l'affaire en tant que preuve. En règle générale, devant les juridictions internationales, la recevabilité d'un élément présenté en preuve est appréciée selon le triple critère de : a) sa pertinence ; b) sa valeur probante ; et c) sa valeur probante par rapport au préjudice qu'il pourrait porter à l'équité du procès[83]. L'élément sera jugé pertinent s'il contribue à rendre un fait plus ou moins probable, et il lui sera reconnu une valeur probante s'il contribue à établir ou à démentir un fait en litige. Dans le cas d'enquêtes non judiciaires, une appréciation similaire à celle de la recevabilité est d'usage. Chaque information devrait être appréciée selon sa fiabilité, sa pertinence et sa valeur probante pour déterminer si elle doit être utilisée et, le cas échéant, comment elle doit l'être afin de dégager des constatations et des conclusions[84].

57. Le poids est la valeur accordée à un élément et la mesure dans laquelle il servira, en définitive, à fonder une constatation ou une conclusion. Sa détermination devrait résulter d'une

79 Par exemple, s'il est coutumier pour les juridictions internationales d'exiger que les faits soient établis « au-delà du doute raisonnable », les commissions d'enquête et les autres organes de cet ordre ont le plus souvent retenu le critère moins exigeant des « motifs raisonnables de penser » pour dégager leurs constatations et conclusions. Pour plus d'informations, voir HCDH, *Commissions d'enquête et missions d'établissement des faits sur le droit international des droits de l'homme et le droit humanitaire international : Orientations et pratiques*, p. 69 et 79.

80 Cour pénale internationale, *Le Procureur c. Jean-Pierre Bemba*, affaire n° ICC-01/05-01/08 A, arrêt relatif à l'appel interjeté par Jean-Pierre Bemba Gombo contre le jugement rendu en application de l'article 74 du Statut par la Chambre de première instance III, 8 juin 2018, Chambre d'appel, *Separate Opinion of Judge Van den Wyngaert and Judge Morrison*, par. 5.

81 Il y a mésinformation lorsque l'information est fausse, mais sans intention de nuire. Par exemple, des personnes qui ne savent pas qu'une information est fausse peuvent décider de la diffuser sur les médias sociaux avec l'intention de rendre service. Il y a désinformation lorsque l'information est fausse et a été délibérément créée ou diffusée avec l'intention expresse de nuire. Les auteurs de désinformation sont habituellement mus par des motifs politiques, financiers, psychologiques ou sociaux. Voir Claire Wardle, *Information disorder: the essential glossary* (Cambridge (Massachusetts), Shorenstein Center on Media, Politics and Public Policy, 2018). Disponible en ligne à l'adresse https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary. pdf?x32994.

82 Id.

83 Selon le Statut de Rome (art. 64 9) a) et 69 4)), la Chambre de première instance de la Cour pénale internationale « peut notamment, à la requête d'une partie ou d'office : Statuer sur la recevabilité ou la pertinence des preuves [...] conformément au Règlement de procédure et de preuve, en tenant compte notamment de la valeur probante de cet élément de preuve et de la possibilité qu'il nuise à l'équité du procès ou à une évaluation équitable de la déposition d'un témoin ».

84 Voir, par exemple, HCDH, *Commissions d'enquête et missions d'établissement des faits : Orientations et pratiques*, en particulier chap. IV.C sur la collecte et l'évaluation des informations.

appréciation holistique dont l'issue déprendra, en partie, des autres informations qui viendraient étayer, corroborer ou contredire le fait en question. Dans de nombreuses procédures judiciaires, la recevabilité et le poids sont appréciés séparément. Dans des situations où ne se pose pas la question de la recevabilité de la preuve, les enquêteurs des droits humains adopteront une approche similaire pour apprécier le poids à accorder à l'information.

58. Les règles de procédure et de preuve applicables aux procédures pénales internationales peuvent se trouver dans les textes constitutifs de chaque juridiction, le plus souvent dans leur règlement de procédure et de preuve. La jurisprudence fournit des indications supplémentaires. Selon la nature de l'enquête, il peut être utile d'obtenir l'avis d'un ou d'une spécialiste, à plus forte raison si l'enquête est destinée à une procédure judiciaire.

59. Les informations de sources ouvertes peuvent combiner des éléments de preuve documentaire et testimoniale. Par exemple, la vidéo d'une personne qui fait des déclarations devra être authentifiée et les déclarations qu'elle contient devront être vérifiées séparément[85]. Aussi faudra-t-il peut-être recourir à des procédés d'authentification de l'élément numérique en tant que document, ou d'évaluation de sa fiabilité et de sa recevabilité en tant qu'élément de preuve testimoniale. Les enquêteurs devraient être au fait des procédés par lesquels chaque catégorie de preuve est traitée devant la juridiction compétente. La preuve documentaire peut souvent s'avérer recevable, même si l'auteur du document n'est pas connu ou en mesure de déposer. Elle peut aussi être recevable sans avoir à être produite par l'intermédiaire d'un témoin en mesure de l'authentifier, pour autant que la partie qui la produit puisse établir de façon claire et précise où et comment elle s'inscrit dans l'affaire concernée[86].

60. Dans les situations où les crimes et violations pourraient engager la responsabilité d'individus plus haut placés dans la structure de commandement, les informations recueillies peuvent être utilisées non seulement pour établir les « faits incriminés » (voir ci-dessous), mais aussi pour établir la forme de participation[87] du ou des auteurs individuels[88]. Un individu peut voir sa responsabilité engagée lorsque chaque

85 Voir Human Rights Center, faculté de droit de l'Université de Californie à Berkeley, *Digital fingerprints: using electronic evidence to advance prosecutions at the International Criminal Court* (Berkeley, 2014). Disponible à l'adresse www.law.berkeley.edu/files/HRC/Digital_fingerprints_interior_cover2.pdf. La preuve par ouï-dire est constituée d'informations dont le témoin qui dépose n'a pas eu directement connaissance. Elle est inadmissible, devant certaines juridictions, à moins qu'elle ne relève d'une exception particulière, et admissible devant d'autres, tout en ne se voyant accorder que peu de poids, dès lors qu'elle ne peut pas être pleinement éprouvée dans le cadre d'un contre-interrogatoire mené par le parquet ou la défense. Selon l'Organisation pour la sécurité et la coopération en Europe, « bien que la preuve par ouï-dire soit généralement inadmissible devant les juridictions de *common law*, à moins de relever de circonstances spéciales, elle n'est frappée d'aucune interdiction devant les juridictions de droit romain ou les tribunaux internationaux ». Voir Organisation pour la sécurité et la coopération en Europe, Mission en Bosnie-Herzégovine, *Investigation Manual for War Crimes, Crimes Against Humanity and Genocide in Bosnia and Herzegovina* (Sarajevo, 2013), p. 26. Disponible à l'adresse www.osce.org/bih/281491?download=true. Malgré cette absence d'obstacles devant les juridictions de droit romain et les tribunaux internationaux, il est de règle générale de considérer la preuve par ouï-dire comme une catégorie particulièrement peu fiable de preuve indirecte auxquels les juges n'accordent souvent que relativement peu de poids.

86 Voir, par exemple, Tribunal pénal international pour l'ex-Yougoslavie, *Le Procureur c. Pavle Strugar*, affaire n° IT-01-42-T, décision relative à l'admissibilité de certains documents, 26 mai 2004, Chambre de première instance II, et *Le Procureur c. Milan Milutinović* et consorts, affaire n° IT-05-87-T, décision relative à la demande d'admission de preuves documentaires présentée par l'accusation, 10 octobre 2006, Chambre de première instance ; Tribunal pénal international pour le Rwanda, *Le Procureur c. Édouard Karemera* et consorts, affaire n° ICTR-98-44-T, *Decision on Joseph Nzirorera's Motion to Admit Documents from the Bar Table: Public Statements and Minutes*, 14 avril 2009, Chambre de première instance III ; Cour pénale internationale, *Le Procureur c. Thomas Lubanga Dyilo*, affaire n° ICC-01/04/-01/06, Decision on the Admission of Material from the « Bar Table », 24 juin 2009 ; Tribunal pénal international pour l'ex-Yougoslavie, *Le Procureur c. Radovan Karadžić*, affaire n° IT-95-5/18-PT, ordonnance relative à la demande de clarification et proposition de l'accusation concernant les lignes directrices sur la conduite du procès, 20 octobre 2009, Chambre de première instance, et *Le Procureur c. Radovan Karadžić*, affaire n° IT-95-5/18-T, *Decision on the Prosecution's First Bar Table Motion*, 13 avril 2010, Chambre de première instance ; Cour pénale internationale, *Le Procureur c. Germain Katanga et Mathieu Ngudjolo Chui*, affaire n° ICC-01/04-01/07, décision relative aux requêtes du Procureur aux fins d'admission de pièces qu'il entend verser directement aux débats, 17 décembre 2010, Chambre de première instance II.

87 Cryer, Robinson et Vasiliev, *An Introduction to International Criminal Law and Procedure*, chap. 15.

88 Voir HCDH, *Who's Responsible? Attributing Individual Responsibility for Violations of International Human Rights and Humanitarian Law in United Nations Commissions of Inquiry, Fact-Finding Missions and Other Investigations* (New York et Genève, 2018). Disponible à l'adresse www.ohchr.org/en/publications/policy-and-methodological-publications/whos-responsible-attributing-individual.

élément d'un crime ou d'une violation, à savoir les actes physiques (l'*actus reus* ou l'élément matériel) et l'état d'esprit de la personne accusée (la mens rea ou l'élément moral), sont établis au niveau de preuve requis. Pour se prononcer sur l'existence de l'infraction, le juge des faits examinera l'information produite au regard de chaque élément de la violation ou du crime. Les enquêteurs devraient être avoir une bonne idée des crimes ou violations qui pourraient être reprochés, des éléments de chacune de ces infractions, des parties à qui elles sont reprochées et selon quelle forme de participation. Dans les affaires de droit pénal international, les praticiens font souvent la distinction entre la preuve relative aux faits incriminés et la preuve relative à la participation à ces faits. Ces deux notions peuvent s'expliciter comme suit :

a) La preuve relative aux faits incriminés tend à établir la commission de l'infraction qui fonde la mise en cause : quel crime a été commis, contre qui, où et quand[89]. Ainsi, en cas d'accusation de meurtre en tant que crime contre l'humanité, toute information tendant à établir qu'il y a eu un meurtre est considérée comme preuve relative aux faits incriminés ;

b) La preuve relative à la participation tend à établir la responsabilité de l'auteur de l'infraction, l'établissement de cette responsabilité étant particulièrement important lorsqu'il ne s'agit pas d'un auteur direct[90]. En d'autres termes, il s'agit de la preuve qui tend à établir le lien entre les faits incriminés et la partie qui en serait responsable. Par exemple, lorsqu'il est reproché à un supérieur hiérarchique d'avoir omis de prévenir ou de punir des violations dont il aurait eu connaissance, la preuve relative à la participation tendra à établir cette connaissance ou le fait que le supérieur exerçait un « contrôle effectif » sur l'auteur direct.

E. Droit à la vie privée et protection des données

61. Le droit à la vie privée est un droit humain fondamental[91]. La protection des données personnelles en est un élément important, consacré par diverses lois relatives à la protection des données[92]. Les lois qui protègent les données et la vie privée revêtent une pertinence croissante pour les enquêtes qui recourent aux informations numériques et à l'informatique. Suit un aperçu de certains aspects du droit humain international à la vie privée et du cadre mondial pour la protection, la sécurité et le partage des données dont les enquêteurs en sources ouvertes devraient être conscients. La confidentialité des informations, en ce qu'elle couvre les informations qui existent ou qui peuvent être déduites concernant une personne, revêt une importance particulière dans l'environnement numérique[93].

62. Les enquêteurs en sources ouvertes doivent respecter les droits humains et devraient être particulièrement sensibles au droit à la vie privée, dont il est souvent question dans le contexte de l'information numérique. Par exemple, la violation du droit à la vie privée

89 Kelly Matheson, *La preuve par vidéo : Guide pratique* (WITNESS, 2016), p. 42. Disponible à l'adresse https://fr.witness.org/portfolio_page/le-guide-de-la-preuve-par-video/.

90 Id.

91 Le droit à la vie privée est inscrit dans de nombreux instruments relatifs aux droits humains ainsi que dans les textes constitutionnels de plus de 130 pays. Voir, par exemple, Déclaration américaine des droits et devoirs de l'homme, art. V ; Convention européenne des droits de l'homme, art. 8 ; Convention américaine relative aux droits de l'homme, art. 11 ; Convention relative aux droits de l'enfant, art. 16 ; Convention internationale sur la protection de tous les travailleurs migrants et des membres de leur famille, art.14 ; Charte africaine des droits et du bien-être de l'enfant, art. 10 ; Charte arabe des droits de l'homme, art. 16 et 21 ; Déclaration des droits de l'homme de l'ASEAN, art. 21. Voir aussi Privacy International, « What is privacy? », 23 octobre 2017. Disponible à l'adresse https://privacyinternational.org/explainer/56/what-privacy.

92 Il y a des lois relatives à la protection des données dans plus de 100 pays et dans de nombreux instruments internationaux et régionaux. Voir, par exemple, Organisation de coopération et de développement économiques, Lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données à caractère personnel ; Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ; Charte des droits fondamentaux de l'Union européenne ; Cadre sur la vie privée de l'Association de coopération économique Asie-Pacifique ; Acte additionnel relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO.

93 Voir, à titre général, A/HRC/39/29, par. 5.

est un des rares motifs sur la base desquels un juge peut exclure des éléments de preuve à la Cour pénale internationale[94]. La vie privée est un fondement et une protection de la dignité humaine et d'autres valeurs essentielles, telles que la liberté d'association et la liberté d'expression. La Cour européenne des droits de l'homme fournit quelques-unes des interprétations les plus robustes des lois relatives à la vie privée, et sa jurisprudence relative aux questions de droits numériques connaît une croissance rapide. Les violations de droits aussi fondamentaux conduiront inévitablement à des contestations de la défense dans les procédures pénales et pourraient même déboucher sur des actions au civil contre les parties qui ont mené l'enquête. Outre les lois relatives à la vie privée, un grand nombre de lois et de règlements relatifs à la protection des données contribuent à la sécurité des données à caractère personnel. Les enquêteurs en sources ouvertes devraient être particulièrement attentifs au règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), et à la conception qui y est retenue de la protection des données personnelles, car ce texte a fixé la barre très haut et d'autres États envisagent d'adopter des dispositions similaires[95]. Il reste que les règlements relatifs à la protection des données varient d'un pays à l'autre, ces variations pouvant être sensibles et parfois même concerner des règles en contradiction directe. Les enquêteurs en sources ouvertes devraient obtenir l'aide de juristes afin de se familiariser avec les lois et règlements relatifs à la protection des données qui les concernent dans les ressorts où ils enquêtent.

63. Enfin, les enquêteurs en sources ouvertes devraient être au fait de l'interdiction générale frappant l'accès non autorisé aux données et aux réseaux. Sont ainsi interdits, par exemple, le fait de se servir d'un mot de passe qui a été divulgué, parce que trouvé dans un ensemble de données volées, pour obtenir des éléments en accès restreint, ou le fait d'accéder sans autorisation à des informations en accès restreint par la tromperie ou d'autres formes de piratage psychologique ou d'ingénierie sociale[96].

F. Autres considérations juridiques pertinentes

64. D'autres lois peuvent s'avérer pertinentes au cours de l'enquête en sources ouvertes. La liste non exhaustive qui suit présente quelques-unes des considérations juridiques dont les enquêteurs en sources ouvertes devraient avoir conscience.

1. Violation des conditions de service

65. Certaines techniques habituelles de l'enquête en sources ouvertes impliquent la violation des conditions d'utilisation d'un site Web ou d'une plateforme. Ainsi, le ratissage de données (scraping) ou l'utilisation d'une identité virtuelle (autre que son identité réelle) sont des violations des conditions de service des plateformes, en particulier des plateformes de

[94] Voir Statut de Rome, art. 69 7).

[95] Le Règlement reconnaît aux personnes physiques des droits en ce qui concerne la protection des données à caractère personnel, la protection à l'égard du traitement des données à caractère personnel et la libre circulation de ces données au sein de l'Union européenne. Des droits similaires sont reconnus par la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et plus remarquablement par le Protocole de 2018 y relatif. La Convention lie non seulement les États membres du Conseil de l'Europe, mais aussi plusieurs autres États.

[96] Selon le National Institute of Standards and Technology, aux États-Unis, l'ingénierie sociale consiste à « tromper un individu pour l'amener à révéler des informations sensibles, en créant avec lui un lien destiné à gagner sa confiance » (Paul A. Grassi, Michael E. Garcia et James L. Fenton, *Digital Identity Guidelines* (Gaithersburg (Maryland, États-Unis), National Institute of Standards and Technology, 2017), p. 54. Voir aussi Michael Workman, « Gaining access with social engineering: an empirical study of the threat », Information Systems Security, vol. 16, nº 6 (2007). Pour plus de détails sur les accès non autorisés ou par tromperie, voir par. 65 ci-dessous. Pour un examen du camouflage de l'identité virtuelle, voir par. 107 ci-dessous.

médias sociaux[97]. Les violations des conditions de service constituent des ruptures de contrat. Les enquêteurs devraient vérifier si elles peuvent également constituer des actes illégaux dans les ressorts où ils travaillent. Il faut mettre en balance l'utilisation d'une identité virtuelle par souci de sécurité et le risque couru, ce faisant, pour rupture de contrat, la mesure la plus commune infligée dans ce cas étant la désactivation de l'accès de l'utilisateur à la plateforme. Cela étant, si les identités virtuelles peuvent être nécessaires pour les activités de recherche et de surveillance des sources ouvertes, comme vu plus haut, elles ne devraient pas être utilisées pour tenter d'obtenir des contenus partagés sur les médias sociaux, alors qu'ils sont d'accès restreint, ou des informations directement auprès d'une personne, en jouant de cette fausse identité. De tels comportements feraient sortir l'enquêteur ou l'enquêtrice du domaine de l'enquête en sources ouvertes, violeraient les principes déontologiques[98] et pourraient enfreindre la loi[99].

2. Lois relatives à la propriété intellectuelle

66. Les enquêteurs devraient être au fait des permissions dont ils pourraient avoir besoin en matière de propriété intellectuelle pour publier, diffuser ou utiliser d'une autre façon, en toute légalité, les informations qu'ils ont collectées dans le cadre de leur enquête. Les lois applicables en la matière peuvent certes varier d'un ressort à un autre, mais dans la plupart des cas, il existe (pour le moins) une certaine protection des droits d'auteur du créateur d'un contenu tel qu'une vidéo, une photo ou un texte partagés en ligne. Le « créateur » s'entend habituellement de la personne qui a effectivement créé le contenu, par exemple, celle qui a pris la photo, enregistré la vidéo ou rédigé le texte original, et non de celle qui l'a téléversé, à cela près qu'il peut s'agir de la même personne. Pour éviter une violation des droits d'auteur, il se peut que le créateur doive consentir à l'usage que l'utilisateur final souhaite faire de son contenu (par exemple, s'il est destiné à un rapport public ou à un récit journalistique), car le consentement du téléverseur, s'il n'est pas aussi le créateur, ne suffit pas habituellement pour éviter d'enfreindre la loi. Encore une bonne raison pour essayer de trouver la source originelle de chaque élément dont les enquêteurs pourraient acquérir. Certaines juridictions (mais pas toutes) prévoient des exceptions à la nécessité d'un consentement, souvent associées à l'« usage loyal » ou à l'« utilisation équitable », lorsque les vidéos, photos, textes ou autres informations sont exploités à certaines fins socialement bénéfiques, comme l'éducation, l'application des lois ou le journalisme. Toutefois, comme ces exceptions sont souvent fort limitées, lorsqu'elles s'appliquent, de sorte qu'il ne faudrait jamais présumer, sans avoir procédé à un examen attentif, que telle ou telle utilisation en bénéficierait. Des dispositions peuvent être prises pour réduire au minimum le risque ou la portée d'une infraction, comme le fait d'incorporer dans le rapport numérique un lien au contenu original, pour ne pas avoir à l'extraire de sa source d'origine, ainsi que le fait de mentionner le créateur ou de n'utiliser qu'une petite portion du contenu, mais encore une fois, en gardant à l'esprit que le résultat dépendra du contexte et de la juridiction. Les informations couvertes par des licences gratuites comme Creative Commons sont utilisables de multiples façons à titre gracieux. Cela étant, en présence d'une telle licence gratuite, il importe de se conformer à ses conditions et de ne pas considérer l'usage du contenu en question comme libre de toute autorisation.

[97] Par exemple, selon les conditions d'utilisation de Facebook, l'utilisateur doit « [d]onner à [son] compte le même nom que celui qu['il] utilise au quotidien », « fournir des informations exactes à [son] sujet » et « [c]réer un seul compte (le sien) et l'utiliser à des fins personnelles ». Voir www.facebook.com/terms.php. L'utilisation d'une fausse identité viole les Règles et politiques de Twitter. Voir « Politique en matière d'identités fallacieuses et trompeuses ». Disponible à l'adresse https://help.twitter.com/fr/rules-and-policies/twitter-impersonation-and-deceptive-identities-policy.

[98] Pour un examen des identités fallacieuses, voir chap. II.C ci-dessus (Principes déontologiques).

[99] Voir chap. III.E ci-dessus (Droit à la vie privée et protection des données).

IV

SÉCURITÉ

SOMMAIRE DU CHAPITRE

- La responsabilité de veiller à la sécurité d'une enquête et des personnes qu'elle touche revient à tous, pas seulement aux professionnels de l'informatique.
- Les considérations de sécurité devraient se manifester à deux égards : a) l'infrastructure, à savoir les matériels, logiciels et réseaux ; b) le comportement, à savoir la façon dont se comportent les enquêteurs et toutes les personnes avec lesquelles ils interagissent.
- L'évaluation de la sécurité devrait s'effectuer sur trois plans, celui de l'organisation, celui de l'enquête/de l'affaire concernée et celui des activités/des tâches envisagées.
- Les mesures de protection devraient être conçues pour atténuer les risques qui ont été relevés dans l'évaluation des risques de l'enquête.
- Les évaluations de sécurité doivent prendre en compte tous types de préjudices, qu'ils soient numériques, financiers, juridiques, physiques, psychosociaux ou relatifs à la réputation.
- Certaines des plus grandes vulnérabilités associées aux enquêtes en sources ouvertes sont liées aux connexions Internet et aux adresses IP, aux appareils et à leurs caractéristiques, ainsi qu'au comportement des utilisateurs.
- Les enquêteurs et les organisations responsables des enquêtes devraient se consacrer de façon continue à des formations en matière de sécurité et déployer des mesures de sécurité qui évoluent en fonction de la nature changeante des menaces et des vulnérabilités.

67. Le présent chapitre propose un aperçu des questions de sécurité en ligne et hors ligne qui se posent dans le cadre des enquêtes en sources ouvertes. Si l'évaluation des menaces et l'atténuation des risques font l'objet du niveau voulu de préparation, d'investissement et d'attention, les enquêteurs en sources ouvertes devraient pouvoir réduire au minimum le risque de préjudice aux personnes, aux données et aux autres avoirs. Une infrastructure de sécurité, matérielle comme logicielle, et des protocoles régissant le comportement des utilisateurs, devraient, dans la mesure du possible, être mis en place préalablement au début de l'enquête, puis évalués régulièrement et mis à jour selon les besoins. La taille et les ressources de l'organisation peuvent avoir une incidence sur les mesures de sécurité accessibles. C'est pourquoi le présent chapitre propose des normes flexibles, prévues pour être adaptées aux besoins propres à chaque organisation et à chaque enquête. Les organisations qui entreprennent des enquêtes à haut risque, telles celles qui concernent des victimes particulièrement vulnérables ou des faits dont les auteurs présumés sont des acteurs étatiques ou des personnes identifiées à titre individuel, devraient s'assurer les services de spécialistes chevronnés de la cybersécurité. Pour être solide, tout cadre de sécurité devrait être assorti d'un dispositif de contrôle indépendant ainsi que d'un programme de formation continue, de sorte que les utilisateurs puissent se tenir au courant des nouvelles avancées technologiques et des meilleures pratiques.

A. Normes minimales

68. Dès lors que l'infrastructure de sécurité et les meilleures pratiques intéressant le comportement des utilisateurs sont en évolution constante, le Protocole propose des principes généraux qui ont pour vocation d'aider les enquêteurs en sources ouvertes à bien étudier les questions de sécurité. Ils doivent en effet assumer la responsabilité de leur propre sécurité, ce qui veut dire évaluer le degré de risque afférent à leur comportement et mettre en place des mesures suffisantes pour atténuer ces risques et s'en protéger. S'il convient d'adapter la gestion de la sécurité à chaque situation, il reste indispensable de se plier à certaines normes minimales garantes du respect des principes de sécurité :

a) Les enquêteurs en sources ouvertes devraient éviter de divulguer à des tiers des éléments susceptibles de révéler leur identité, celle de leur organisation et celle de n'importe quel partenaire et source, à moins qu'il ne s'agisse d'un objectif ou d'une obligation de l'enquête elle-même. Ils devraient par conséquent préserver leur anonymat en ligne et veiller, dans toute la mesure possible, à ce que leurs activités n'y soient pas attribuables ;

b) Les enquêteurs en sources ouvertes devraient effectuer leurs recherches en ligne en partant du principe que ces activités pourraient être surveillées et analysées par des tiers. Ils devraient par conséquent se comporter d'une manière qui corresponde à leur identité virtuelle, qui ne révèle ni leur identité effective ni le fait qu'ils enquêtent, et qui préserve du danger leurs sources humaines et les autres parties concernées ;

c) Les enquêteurs en sources ouvertes devraient être conscients du fait que la surexploitation d'une seule source d'information en ligne, comme un site particulier, peut accroître le risque de surveillance et d'analyse par une tierce partie. Ils devraient par conséquent mettre en place des pratiques, telle la diversification des sources numériques, qui tendent à réduire au minimum cette possibilité ;

d) Les enquêteurs en sources ouvertes devraient éviter d'adopter des comportements repérables ou prévisibles, telle l'application répétée de schémas de recherche à partir d'appareils identifiables, qui pourraient mettre des tiers sur la piste de leurs enquêtes et les exposer à l'hameçonnage et à d'autres formes d'ingénierie sociale[100] ;

e) Les enquêteurs en sources ouvertes devraient maintenir une séparation entre leurs tâches professionnelles et leurs activités en ligne à des fins personnelles. Les comptes en ligne à usage personnel

[100] Pour une explication de l'hameçonnage et de l'ingénierie sociale, voir ci-dessous.

et, dans la mesure du possible, le matériel personnel ne devraient pas être utilisés pour effectuer des recherches professionnelles, et le matériel professionnel ne devrait jamais être utilisé pour mener des activités personnelles en ligne[101] ;

f) Les enquêteurs en sources ouvertes qui mènent plusieurs enquêtes à la fois ne devraient pas entremêler ces travaux. Ils devraient fixer des heures de début et de fin de travail distinctes pour chaque enquête, conserver les données et les documents relatifs à chaque enquête en des lieux séparés et utiliser différentes identités virtuelles, selon les besoins[102] ;

g) Les enquêteurs en sources ouvertes devraient utiliser des systèmes ou des environnements techniques conçus pour être les moins sensibles possible à l'introduction de logiciels malveillants ou à d'autres influences perturbatrices qui pourraient se manifester au cours de leurs activités.

B. Évaluations de la sécurité

69. Pour être en mesure de se doter d'un cadre de sécurité adéquat et efficace, les enquêteurs en sources ouvertes doivent comprendre les principaux éléments de la cybersécurité et de la gestion des risques. Ils doivent également être en mesure de déterminer les actifs à protéger et les préjudices à craindre, et pouvoir évaluer les menaces, les risques et les vulnérabilités.

70. Le risque s'entend de la possibilité qu'une ressource soit perdue, endommagée ou détruite par une menace qui tire parti d'une vulnérabilité pour se réaliser. Chacun de ces termes est défini ci-dessous. Comme les enquêtes en sources ouvertes menées sur Internet utilisent des méthodes de collecte de l'information différentes de celles utilisées par les enquêtes traditionnelles, elles présentent aussi des risques de types différents. Le recensement et l'évaluation de ces risques est une partie importante de la planification et de la préparation d'une enquête. Parmi les risques communément associés aux enquêtes en sources directes, on notera : les moyens techniques, la connaissance de l'enquête et le soutien de certaines entités qui pourraient permettre à la cible de l'enquête de s'y soustraire ou de l'induire en erreur ; la configuration technique problématique de l'environnement en ligne utilisé pour l'enquête qui pourrait révéler des informations susceptibles de compromettre l'enquête ; les logiciels ou programmes malveillants qui pourraient compromettre les systèmes informatiques, les activités, ou les données collectées de l'enquêteur ou l'enquêtrice, ou dévoiler son identité ; les dispositifs techniques tels que les traqueurs, les cookies, les pixels espions et les procédés analytiques qui peuvent compromettre les activités d'enquête.

71. La section suivante explique les termes clefs et leur application aux enquêtes en sources ouvertes, établissant ainsi un plan d'action pour réaliser une évaluation des menaces et des risques.

1. Actifs

72. Tout ce qui nécessite protection est un actif, qu'il s'agisse d'une personne[103], d'un bien ou d'une information. Dans le contexte des enquêtes en sources ouvertes, les personnes à protéger peuvent être les enquêteurs ou les équipes d'enquête, de même que toute personne avec qui les enquêteurs ou les équipes d'enquête travaillent (les collègues au sein de l'organisation et les partenaires externes, sur place ou sur le terrain), les auteurs ou les sources de l'information, les témoins, les victimes, les auteurs présumés des faits et les « spectateurs ». Les biens sont constitués d'éléments corporels et incorporels auxquels se rattache une valeur[104]. Les actifs corporels comprennent les immeubles, les équipements et

[101] Si l'utilisation du matériel personnel est inévitable, les enquêteurs devraient mener leurs activités professionnelles et personnelles dans des environnements en ligne distincts, par exemple en utilisant une machine virtuelle pour leurs enquêtes.

[102] Outre qu'elles réduisent au minimum le risque de confondre les enquêtes, ces pratiques sont utiles pour préserver les chaînes de contrôle.

[103] Les personnes ne sont considérées comme des « actifs » que dans le cadre des évaluations de sécurité.

[104] Voir Threat Analysis Group, « Threat, vulnerability, risk – commonly mixed up terms ». Disponible à l'adresse www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms.

les documents, tandis que les actifs incorporels comprennent la réputation et les informations exclusives qui peuvent notamment se présenter sous la forme de données numériques, de métadonnées, de bases de données, de code source de logiciels et de registres.

2. Préjudice

73. Le préjudice résulte d'un dommage ou d'une blessure de nature physique ou mentale causé à un actif, ou de la destruction de tel actif. Il peut être numérique, financier, juridique, physique, psychosocial ou relatif à la réputation.

a) Préjudice numérique

74. Il y a préjudice numérique lorsqu'un dommage a été causé à l'information ou à l'infrastructure numériques. Il peut s'agir de la destruction de données, de leur manipulation et de l'impossibilité d'y accéder, ou de la perturbation des services fournis par les systèmes et plateformes informatiques.

b) Préjudice financier

75. Le préjudice financier peut avoir plusieurs sources, telles que les effets juridiques d'une enquête ou son incidence sur la réputation. Il peut toucher aussi bien les enquêteurs que leurs cibles et les tiers qui ont assisté aux faits. Il peut en outre survenir lorsque des enquêteurs n'ont pas bien évalué le coût d'une enquête sur le long terme.

c) Préjudice juridique

76. Les enquêteurs en sources ouvertes peuvent voir leur responsabilité juridique engagée du fait de ce qu'ils font dans le cadre de leurs travaux et de ce qu'ils produisent à l'issue de ces travaux. Ils devraient connaître les limites et les ramifications juridiques de leurs activités, de sorte à réduire au minimum la responsabilité juridique qui pourrait en découler pour eux-mêmes ou des tiers. Les enquêtes peuvent également causer un préjudice juridique à celles et ceux qui en font l'objet, voire aux spectateurs des faits visés, lorsque ceux-ci sont impliqués dans des irrégularités juridiques mises au jour par l'enquête[105].

d) Préjudice physique

77. Le préjudice physique s'entend des dommages occasionnés aux personnes et aux biens. Bien que les enquêteurs en sources ouvertes travaillent habituellement dans des bureaux ou chez eux, et non sur le terrain, il importe d'évaluer les préjudices physiques qui pourraient résulter de leurs activités en ligne. De fait, ce que l'on fait dans le cyberespace peut avoir des conséquences dans le monde réel. C'est un fait dont les enquêteurs devraient être conscients et auquel ils devraient être préparés. Ainsi les enquêteurs en sources ouvertes devraient-ils savoir quels collègues, quels utilisateurs en ligne dans les pays visés ou quelles autres personnes se trouvent dans des environnements peu sûrs où ils risquent de subir des préjudices physiques par suite du comportement en ligne d'un enquêteur ou d'une enquêtrice. Les principes déontologiques – et la loi dans certains cas – imposent aux enquêteurs un devoir de protection[106] vis-à-vis d'autrui. Il s'agit de veiller à ce que celles et ceux qui risquent de subir un préjudice physique ne soient pas exposés à un danger accru du fait des activités d'enquête. Les risques physiques devraient être pris en compte dans le cadre de l'évaluation complète des menaces avant le début du travail, et réévalués tout au long de l'enquête.

e) Préjudice psychosocial

78. Le préjudice psychosocial peut aller de la détresse psychologique au traumatisme, et peut affecter tout membre d'une équipe d'enquête et toute personne autrement mise à contribution ou affectée par une enquête, y compris celles et ceux qui en font l'objet ou qui sont de simples spectateurs. Outre qu'il est moralement et déontologiquement important pour les enquêteurs de veiller à leur propre protection et à celle d'autrui contre les préjudices psychologiques, les êtres humains peuvent parfois aussi devenir les chaînons les plus vulnérables du fonctionnement d'une

[105] Voir aussi les chapitres IV.E et IV.F ci-dessus pour un examen plus approfondi des enjeux juridiques.

[106] Statut de Rome, art. 54 1) b).

organisation. La personne qui peine sur le plan psychologique peut devenir particulièrement vulnérable. Sa situation risque de créer des occasions pour les acteurs de menaces et exposer la sécurité physique et numérique de l'enquête à d'autres dangers, surtout si son état a un effet négatif sur la façon dont le travail est accompli, de sorte que, par exemple, les protocoles de sécurité ne sont plus suivis avec la rigueur voulue. Le fait de visionner de nombreuses vidéos aux contenus violents ou perturbants peut engendrer une détresse psychologique ou un traumatisme qui nécessitent des soins professionnels. Le traumatisme secondaire peut se manifester de diverses façons, parmi lesquelles les changements de comportement, d'humeur, d'habitudes alimentaires et de consommation d'alcool, les difficultés à dormir ou l'envie de dormir plus que de coutume, et les cauchemars plus fréquents[107]. Des stratégies d'atténuation des préjudices sont décrites dans la section consacrée au plan de résilience et aux autosoins dans le cadre de la préparation de l'enquête[108].

f) Atteinte à la réputation

79. Le risque d'atteinte à la réputation est particulièrement élevé pour les enquêteurs ou pour les organisations qui les emploient si, dans le cadre d'une enquête en sources ouvertes, les enquêteurs publient des informations erronées, contreviennent aux règles déontologiques ou, plus généralement, produisent des contenus problématiques. Les sujets des enquêtes peuvent eux aussi subir une atteinte à la réputation, sous la forme d'une stigmatisation lorsque le comportement qui leur est reproché est rendu public. Cette possibilité est particulièrement préoccupante lorsque les accusations portées contre des personnes ou des organisations s'avèrent ensuite sans fondement.

3. Mesures de protection

80. Les mesures de protection sont des dispositions prises pour prévenir les vulnérabilités ou les réduire autant que possible. Elles peuvent être physiques, technologiques et directrices. Les mesures physiques peuvent consister à verrouiller les immeubles, les pièces et le mobilier où sont conservés les documents sensibles. Les mesures technologiques consistent notamment à recourir aux mots de passe, au chiffrement et à l'authentification multifacteurs, ou à contrôler l'accès aux systèmes de données. Les mesures directrices comprennent les règles internes et externes, les lois et les mécanismes d'application, par exemple les règles qui proscrivent l'envoi des résultats d'un travail interne d'une adresse électronique professionnelle à une adresse électronique privée ou les directives contre l'utilisation de comptes de médias sociaux privés sur un ordinateur de travail.

4. Menaces

81. Une menace est un fait contre lequel les actifs doivent être protégés. Elle s'entend de tout ce qui exploite une vulnérabilité, intentionnellement ou accidentellement, et conduit à la subtilisation, l'endommagement ou la destruction d'un actif. Elle peut provenir de l'intérieur ou de l'extérieur d'une organisation ou d'une enquête et être exécutée par un individu, un groupe, une entité ou un réseau. Les enquêteurs en sources ouvertes devraient avoir connaissance des menaces suivantes, parmi d'autres.

a) Attaques par déni de service distribué

82. Les attaques par déni de service distribué sont des cyberattaques conçues pour perturber la capacité de leur cible d'accéder à une machine ou à un réseau. Les actifs qui sont en

[107] Voir Dart Center for Journalism and Trauma, « Working with traumatic imagery », 12 août 2014 (disponible à l'adresse https://dartcenter.org/content/working-with-traumatic-imagery) ; Sam Dubberley, Elizabeth Griffin et Haluk Mert Bal, *Making Secondary Trauma a Primary Issue: A Study of Eyewitness Media and Vicarious Trauma on the Digital Frontline* (Eyewitness Media Hub, 2015) (disponible à l'adresse http://eyewitnessmediahub.com/research/vicarious-trauma) ; Sam Dubberley et Michele Grant, « Journalism and vicarious trauma: a guide for journalists, editors and news organisations » (First Draft News, 2017) (disponible à l'adresse https://firstdraftnews.org/wp-content/uploads/2017/04/vicarioustrauma.pdf) ; Center for Human Rights and Global Justice, « Human Rights Resilience Project launches new website », 21 mai 2018 (précédemment disponible à l'adresse https://chrgj.org/2018/05/21/human-rights-resilience-project-launches-resources-for-resilience-website) ; Keramet Reiter et Alexa Koenig, « Reiter and Koenig on challenges and strategies for researching trauma » (Palgrave MacMillan) (disponible à l'adresse www.palgrave.com/gp/blogs/social-sciences/reiter-and-koenig-on-researching-trauma).

[108] Voir chap. V.D ci-dessous pour plus d'informations sur les autosoins.

interface avec le public, comme les sites Web et les portails d'accès à distance, devraient être protégés par un système visant à contrer de telles attaques. Il faudrait aussi mettre en place et en œuvre un système qui, en cas d'attaque, enregistre toutes les actions effectuées et tous les acteurs concernés.

b) Attaques par hameçonnage

83. L'hameçonnage est une tentative frauduleuse d'obtenir des informations sensibles, telles que les noms d'utilisateur, les mots de passe et les données de cartes de crédit, en usurpant une identité digne de confiance dans une communication électronique[109]. L'hameçonnage et son équivalent téléphonique sont utilisés pour obtenir des informations confidentielles ou harceler l'enquêteur ou l'enquêtrice. Les comptes personnels étant généralement plus susceptibles aux attaques de ce genre que les comptes professionnels, l'usage des premiers peut compromettre les travaux d'enquête ou leur résultat.

c) Attaques de l'homme du milieu

84. Les attaques de l'homme du milieu sont un type de cyberattaque par lequel des acteurs malveillants s'introduisent dans une conversation entre deux parties, se font passer pour les deux parties et obtiennent des informations que les deux parties se destinaient l'une à l'autre[110]. Ce type d'attaque permet à un acteur malveillant d'intercepter, d'envoyer ou de recevoir des données qui étaient destinées à quelqu'un d'autre ou qui ne devaient pas être expédiées du tout, les parties concernées ne se rendant compte de la supercherie que lorsqu'il est trop tard[111].

d) Ingénierie sociale

85. L'ingénierie sociale consiste à manipuler psychologiquement des personnes pour les amener à agir de façon potentiellement dommageable, comme la divulgation d'informations personnelles. L'ingénierie sociale prend de nombreuses formes, comme l'hameçonnage ciblé ou le harponnage[112]. Comme les tactiques d'ingénierie sociale s'adaptent et évoluent sans cesse, les enquêteurs devraient se former continuellement à la détection et à l'évitement des attaques de ce type.

e) Logiciels malveillants

86. Les logiciels malveillants sont des programmes informatiques conçus pour s'infiltrer dans les ordinateurs et les endommager à l'insu des utilisateurs. Il en existe plusieurs types dont les mouchards ou logiciels espions et les rançongiciels ou logiciels rançonneurs.

5. Acteurs malveillants

87. L'acteur malveillant ou l'acteur d'une menace est une personne ou une entité qui se rend responsable d'un fait qui a, ou qui peut avoir, une incidence sur la sûreté ou la sécurité d'une autre entité ou d'un autre acteur. Dans les enquêtes sur les crimes internationaux et sur les violations des droits humains internationaux, les acteurs des menaces seront probablement les auteurs présumés des faits, les sujets de l'enquête, notamment les gouvernements ou leurs partisans. Il importe que les enquêteurs en sources ouvertes repèrent les acteurs malveillants potentiels et jaugent leurs capacités et la probabilité qu'ils lancent des attaques.

6. Vulnérabilités

88. Une vulnérabilité est une faiblesse ou une lacune dans les mesures de protection. Elle peut exister dans la sphère numérique comme dans la sphère physique. Dans le cas des activités en ligne, elle peut se présenter sous la forme d'une faiblesse dans le dispositif de sécurité qui pourrait être exploitée pour accéder sans autorisation à tel ou tel actif, elle pourrait résulter d'un défaut de sécurité dans un logiciel ou d'une conception peu sûre, ou encore être le fait d'utilisateurs ou de programmes

[109] Voir Phishing.org, « What is phishing? ». Disponible à l'adresse www.phishing.org/what-is-phishing.

[110] Voir Veracode, « Man in the middle (MITM) attack ». Disponible à l'adresse www.veracode.com/security/man-middle-attack.

[111] Id.

[112] L'hameçonnage ciblé ou harponnage est une pratique frauduleuse consistant à envoyer des messages électroniques provenant apparemment de sources bien connues ou dignes de confiance à des personnes précises afin de les amener à révéler des informations confidentielles.

auxquels des droits d'accès excessifs ont été accordés. Hors ligne, les vulnérabilités peuvent aussi être dues aux faiblesses affectant les personnes, notamment lorsqu'au sein d'une équipe, une personne est exposée au chantage ou à la coercition, ou devient vulnérable par suite de sa surexposition à des contenus perturbants ou à d'autres conditions de travail difficiles[113]. Des vulnérabilités peuvent également apparaître lorsqu'une partie est informée de l'existence d'une enquête à son encontre ou que la portée d'une enquête est révélée. Enfin, les vulnérabilités de sécurité peuvent provenir de menaces externes, comme l'apparition de nouveaux logiciels malveillants ou de nouveaux virus, dont les enquêteurs devraient être conscients. Ce sont des types de vulnérabilités qui devraient être pris en compte par la cartographie de la sécurité et l'évaluation des risques.

89. Les enquêteurs en sources ouvertes devraient aussi être conscients de la présence en ligne des vulnérabilités suivantes.

a) Témoins de connexion ou cookies

90. Un témoin de connexion ou cookie est un petit fichier qui, souvent envoyé par l'intermédiaire d'un site Web, s'installe dans la mémoire ou s'écrit sur le disque d'un ordinateur pour être utilisé par un navigateur. Les cookies sont souvent nécessaires au fonctionnement correct d'un site Web. Ils permettent, par exemple, l'enregistrement des préférences et des identifiants des utilisateurs du site pour leur éviter d'avoir à saisir ces données à chaque visite subséquente. Ils sont conçus de sorte à pouvoir emmagasiner des données importantes, et souvent sensibles, concernant les visiteurs et leurs visites. Certains sont devenus des outils centralisés capables de rassembler des données qui serviront à dresser le tableau des intérêts et des habitudes de navigation de l'utilisateur. Un cookie peut rester sur un ordinateur jusqu'à son expiration ou sa suppression par l'utilisateur.

b) Traqueurs

91. Un traqueur est un type de cookie qui exploite la capacité d'un navigateur de conserver une trace des pages visitées, des critères de recherche saisis, etc. Les traqueurs sont des témoins de connexion permanents qui maintiennent un relevé continu du comportement du visiteur d'un site Web. Dans leur forme la plus simple, les traqueurs assignent une identité unique au navigateur d'un utilisateur et associent ensuite à cette identité toutes les activités de navigation et de recherche subséquentes (critères de recherche, pages visitées, séquence des pages visitées, etc.). Ce qui donne au propriétaire du traqueur la possibilité de mettre en conjonction les visites précédentes et subséquentes d'un site (ou d'une série de sites affiliés) afin de dresser un tableau détaillé des utilisateurs et de leurs habitudes de navigation. Les traqueurs sont souvent incorporés dans des publicités ensuite diffusées à de nombreux sites Web, multipliant ainsi les occasions de saisie des activités et des comportements des internautes. Même la visite d'un site « de confiance » peut se solder par l'installation de traqueurs sur les ordinateurs des utilisateurs et le suivi de leurs futures activités.

c) Pixels espions ou pixels invisibles

92. Le pixel espion ou pixel invisible est un dispositif de pistage des activités et des comportements des utilisateurs constitué d'un petit élément graphique (souvent invisible, de la taille d'un seul pixel transparent) discrètement inséré dans une page Web. Lorsque le pixel espion est capté par un navigateur, des informations concernant le navigateur et l'ordinateur qui y est associé sont renvoyées à une tierce partie. Les pixels espions peuvent être utilisés avec des cookies pour déclencher la collecte de données, reconnaître les utilisateurs et enregistrer leurs habitudes de navigation. Les pixels espions sont étroitement liés aux sites de médias sociaux, dont le fonctionnement repose dans une mesure importante sur l'établissement de relations et de réseaux. Enfin, ils peuvent être utilisés

[113] Voir chap. V.D ci-dessus pour plus d'informations sur la résilience et les autosoins.

dans des messages électroniques en HTML pour collecter et transmettre des informations concernant l'identité d'un utilisateur et accéder à tout cookie précédemment installé sur son ordinateur.

d) Autres programmes et scripts

93. Un nombre croissant de sites Web recourent à de petits programmes qui, téléchargés par le navigateur du visiteur, ont la capacité d'emmagasiner des informations concernant la visite. Ces programmes peuvent influencer la façon dont le site Web se présente, dont il réagit aux informations saisies et dont le navigateur répond au site. Ils peuvent également recueillir des informations sensibles concernant les identifiants du visiteur, ses activités, etc. Les données peuvent être collectées de façon permanente et envoyées à une tierce partie.

C. Considérations relatives à l'infrastructure

94. L'infrastructure s'entend des structures, installations et systèmes – logiciels et matériels compris – nécessaires pour mener des enquêtes en sources ouvertes. Elle devrait fournir des mesures de sécurité suffisantes (et donc avoir été dotée de mesures de sécurité suffisantes) pour protéger et préserver les actifs et les données d'une organisation. Sa résilience devrait être assurée par des mesures d'atténuation mises en place pour assurer la continuité des opérations dans l'un quelconque des cas suivants :

a) La perturbation ou la perte d'une connexion Internet ;

b) La perturbation ou la perte de l'accès à des données stockées ;

c) La perte, la contamination ou la destruction de données ;

d) La perturbation ou la perte de services logiciels ;

e) L'endommagement ou la perte de matériel ;

f) L'accès non autorisé à des appareils ;

g) L'accès non autorisé à un réseau ;

h) La suppression ou la manipulation accidentelles de données ;

i) La destruction ou la manipulation intentionnelles de données ;

j) La fuite ou la « prise en otage » de données.

95. L'architecture nécessaire se définit en fonction de l'ampleur des activités d'enquête à mener en ligne, de la nature de l'enquête et de son objet, ainsi que des moyens financiers disponibles pour construire, maintenir et modifier l'infrastructure selon les besoins.

1. Infrastructure

96. L'infrastructure utilisée pour les enquêtes en sources ouvertes comprendra au moins les éléments passés en revue ci-après, auxquels viendront s'ajouter des éléments propres aux différentes stratégies d'enquête.

a) Appareils

97. Les enquêteurs en sources ouvertes doivent disposer d'appareils qui leur permettent d'accéder aux contenus en ligne, tels un ordinateur de bureau, un ordinateur portable, une tablette ou un smartphone. Ces appareils devraient être protégés par des mots de passe, le chiffrement intégral des disques et, idéalement, l'authentification multifacteur[114], et ils devraient régulièrement faire l'objet de copies de secours. Lorsqu'il n'est pas utilisé, ce matériel devrait être entreposé de façon sûre, seuls l'utilisateur et le personnel autorisé y ayant accès. Les appareils personnels ne devraient pas être utilisés à des fins professionnelles. De même, les appareils servant aux enquêtes ne devraient pas être utilisés à des fins personnelles, pour éviter qu'un lien puisse être établi entre les activités personnelles menées sur les médias sociaux et

[114] L'authentification multifactorielle est un dispositif de sécurité améliorée qui requiert de l'utilisateur qu'il présente deux types d'identifiants pour se connecter à un compte, par exemple, un mot de passe et un identifiant biométrique (empreinte digitale) ou une carte à puce. Voir National Institute of Standards and Technology (États-Unis), « Back to basics: multi-factor authentication (MFA) ». Disponible à l'adresse www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication.

les identités virtuelles entretenues dans le cadre des enquêtes[115].

b) Connexion Internet

98. Idéalement, les enquêteurs disposeront d'une connexion Internet de bonne qualité, stable et privée. Bien que pratique, le Wi-Fi public gratuit – y compris les réseaux semi-privés tels que ceux mis à disposition par les hôtels ou les cafés Internet – est très peu sûr et ouvert à de nombreuses menaces, dont la principale est la possibilité pour un pirate informatique (hacker) de se placer entre l'utilisateur et le point de connexion. L'utilisation d'une borne Wi-Fi personnelle, protégée par un mot de passe, nécessite un investissement financier, mais est essentielle pour la sécurité des activités d'enquête menées en ligne. En outre, bien que cela ne soit pas toujours du ressort de l'enquêteur ou de l'enquêtrice en ligne, une connexion Internet de bonne qualité et stable est préférable à la fois pour des raisons de fonctionnalité et de sécurité. Les enquêteurs qui utilisent un réseau privé virtuel (réseau VPN) en combinaison avec une connexion instable devraient mettre en place un dispositif de sécurité pour qu'en cas d'interruption de la connexion, l'adresse IP ne soit pas révélée.

c) Navigateurs

99. Le navigateur est l'un des principaux outils utilisés pour enquêter en ligne. Il permet d'effectuer des recherches parmi les sites Web publiés sur Internet, d'accéder à ces sites et de les interroger. Principale interface entre les enquêteurs et Internet, il n'est pourtant pas rare qu'il soit omis des sources possibles de risques. En mutation constante, les navigateurs modernes sont dotés d'une grande variété de fonctionnalités qui répondent à une multitude de besoins. Ils sont aussi une cible de choix pour les activités de surveillance et les attaques visant des adversaires, car il est relativement aisé de détourner ou d'ajouter des fonctionnalités à ces fins. Le navigateur jouit d'un accès simultané à Internet et à l'ordinateur, ce qui lui confère le potentiel de relever des informations concernant l'utilisateur. La fuite de données par l'entremise d'un navigateur peut être suffisante pour alerter une partie qu'elle est sous enquête. Plusieurs fonctions sont intégrées dans les navigateurs modernes, et une multitude d'autres – les addiciels – peuvent y être ajoutées. Individuellement ou collectivement, elles peuvent occasionner la fuite de données et conduire à la découverte d'une enquête, de l'identité d'un enquêteur ou d'une enquêtrice, ou encore d'une piste d'investigation et des activités de recherche y associées. Les navigateurs sont aussi, par défaut, capables de télécharger et d'exécuter des programmes informatiques provenant de sites Web. Alors que les enquêteurs peuvent ne pas se rendre compte de la présence ou de la fonction d'un programme, celui-ci peut altérer le contenu numérique qui leur parvient, accéder à des fonctionnalités et des données sur leurs ordinateurs et même amener les ordinateurs à se comporter d'une façon différente de celle qui était prévue. Les enquêteurs en sources ouvertes devraient s'efforcer de réduire au minimum ces risques en veillant à n'utiliser que des navigateurs sûrs, actualisés et régulièrement vérifiés, et en utilisant des logiciels et des plugiciels capables d'atténuer certains des risques décrits ci-dessus[116].

2. Mesures de sécurité

100. Ces éléments essentiels d'infrastructure peuvent être utilisés pour découvrir qui sont les utilisateurs et où ils se trouvent. Afin de se conformer aux principes d'anonymat et de non-attribution, les enquêteurs devraient adopter les stratégies présentées ci-après pour camoufler leurs connexions Internet. Ce sont des stratégies visant à masquer le lieu et l'adresse IP associés à une machine, et à camoufler celle-ci en masquant les aspects de ses fonctions, de son système d'exploitation et de son navigateur qui permettent de l'identifier.

[115] Cette recommandation peut s'avérer difficile à suivre en cas de déplacement, car de nombreux enquêteurs emporteront leurs appareils de travail, mais voudront ou devront s'occuper de questions personnelles en dehors des heures de travail. Aussi faudrait-il que les organisations qui mènent des enquêtes en sources ouvertes mettent au point des règles raisonnables pour encadrer les voyages du personnel d'enquête sur ce point.

[116] Pour des orientations actualisées concernant les navigateurs et d'autres mesures de sécurité opérationnelle, se référer au Computer Security Resource Center du National Institute of Standards and Technology (États-Unis, https://csrc.nist.gov/).

a) Camouflage de la connexion

101. L'adresse IP recèle des informations qui peuvent être utilisées contre l'infrastructure d'une organisation. Les enquêteurs en sources ouvertes devraient par conséquent s'efforcer de recourir à des réseaux VPN, à des serveurs mandataires (serveurs proxy) ou à d'autres logiciels destinés à masquer les adresses IP de leurs ordinateurs, de sorte que les adresses visibles sur Internet ne pourront être associées ni à l'enquêteur ou à l'enquêtrice ni à son organisation. Les réseaux VPN créent également un tunnel de communication chiffré entre l'ordinateur de l'enquêteur ou de l'enquêtrice et le serveur du réseau. Ainsi tout réseau intermédiaire ou autre par lequel la connexion pourrait passer ne verraient-ils que des données chiffrées, ce qui constitue une couche de protection supplémentaire. Cela étant, l'usage de certains réseaux VPN étant bloqué par certains pays et sites Web, il peut rendre des activités d'enquête suspectes aux yeux de tierces parties. Idéalement, les réseaux VPN devraient permettre aux enquêteurs d'utiliser de multiples adresses IP et de passer rapidement de l'une à l'autre si nécessaire. Les adresses IP ne devraient pas se rapporter à un seul et même pays, mais être réparties entre de multiples endroits dans le monde.

b) Camouflage de la machine

102. Afin de masquer certaines fonctions qui pourraient être utilisées pour identifier les utilisateurs, les enquêteurs peuvent se servir de machines virtuelles, qui sont des logiciels ou des systèmes d'exploitation qui se comportent comme des ordinateurs distincts. L'utilisation d'une machine virtuelle revient essentiellement à créer un nouvel ordinateur au sein de l'ordinateur existant, dans un environnement tout à fait séparé du reste de la machine. La machine virtuelle est aussi capable d'effectuer des tâches, notamment d'exécuter des applications et des programmes comme le ferait un ordinateur à part entière[117] ; l'enquêteur ou l'enquêtrice qui s'en sert apparaît ainsi comme un acteur différent en ligne. Lorsqu'ils utilisent une machine virtuelle, les enquêteurs ont à leur disposition un système qui leur permet de modifier le navigateur, l'agent utilisateur, les logiciels, les ports ouverts, le système d'exploitation et d'autres informations concernant la machine afin de se présenter comme un sujet différent à chaque fois qu'ils se mettent en ligne. Idéalement, l'infrastructure devrait permettre à l'enquêteur ou à l'enquêtrice d'utiliser une machine virtuelle qui masque la machine dont il se sert effectivement. Les machines virtuelles peuvent être détruites et recréées, restaurées à partir d'un point précédent, configurées de différentes façons, reproduites pour de nouveaux dossiers ou conservées pour un usage ultérieur. Les enquêteurs ont également la possibilité d'opter pour la solution plus laborieuse, mais aussi relativement efficace, de modifier leur apparence manuellement, en utilisant des navigateurs différents chaque fois qu'ils vont en ligne, en modifiant les réglages pour rendre l'empreinte numérique de leur machine moins distinctive et en recourant à des plugiciels qui empêchent le pistage.

3. Autres éléments d'infrastructure

103. Avant d'entamer leur travail, les enquêteurs devraient envisager la mise en place d'autres éléments pour protéger leurs réseaux et leurs infrastructures, notamment :

a) Des systèmes de sauvegarde ;

b) Des systèmes de journalisation ;

c) Des systèmes de stockage séparés et des lieux de stockage adéquats pour recueillir les éléments relevés pendant les recherches. Afin de protéger les données de l'extérieur, les organisations devraient disposer de plateformes (telles que des répertoires des éléments de preuve, des bases de données ou d'autres systèmes de gestion des informations) qui restent séparées des réseaux principaux. Ces plateformes devraient contenir deux parties principales : l'une connectée à Internet et l'autre déconnectée. Dans certains cas, il peut s'avérer opportun de transférer dès

[117] Voir Techopedia, « Virtual machine (VM) », 21 mai 2020. Disponible à l'adresse www.techopedia.com/definition/4805/virtual-machine-vm.

que possible des données de l'infrastructure connectée à un réseau ou répertoire plus sécurisé, pour que les informations puissent être examinées en toute sécurité.

D. Considérations relatives aux utilisateurs

104. L'utilisateur est un des éléments les plus faibles du dispositif de sécurité. Même en présence d'une infrastructure parfaite, les principes de sécurité ne seront pas appliqués sans une adaptation du comportement des utilisateurs. Celle-ci se réalisera par l'application régulière de mesures de formation et de contrôle. La sécurité est la responsabilité de tous. Les individus ne devraient pas entreprendre des activités qui pourraient mettre des données ou des personnes en danger sans avoir été adéquatement formé à l'atténuation de ces risques. Les enquêteurs devraient être formés de façon à pouvoir déterminer quel comportement doit être adopté pour mener telle ou telle activité en ligne.

105. L'anonymat peut aider à réduire le risque de subir des préjudices si un acteur malveillant tente de remonter vers le réseau ou l'utilisateur qui est à l'origine d'une activité[118]. Toute activité en ligne étant exposée au retraçage par des tiers, les enquêteurs devraient partir du principe que cette menace existe dès lors qu'ils agissent en ligne. Les cibles les plus communes d'un retraçage sont les adresses IP, les navigateurs et la résolution des écrans (pour identifier les appareils), ainsi que le temps de navigation et les activités menées sur les sites Web (telles que les termes de recherche saisis ou les pages visitées). L'acteur malveillant peut tenter d'identifier la source des activités d'enquête menées en ligne. S'il y a tentative de retraçage, l'auteur de la menace devrait être détourné du lieu où se trouvent effectivement les enquêteurs ou les entités responsables de l'enquête, ainsi que de l'identité de ces parties. Cette parade est réalisable en prenant des dispositions pour que les points d'accès des activités d'enquête semblent se situer ailleurs, grâce à un réseau VPN par exemple, ou pour que les acteurs de l'enquête semblent être quelqu'un d'autre, grâce à la création et à l'utilisation d'identités virtuelles[119].

106. Le fait de masquer la connexion et la machine utilisées dans une enquête en ligne constitue une protection importante, qui peut toutefois être compromise si les utilisateurs se font connaître en s'identifiant sur un site Web ou, par exemple, en fournissant des renseignements personnels pour s'inscrire ou se connecter à une plateforme de médias sociaux ou à un autre service privé. Les enquêteurs ne devraient jamais utiliser de comptes privés pour enquêter ni se connecter à des comptes privés au moyen du navigateur qui sert aux enquêtes. Certains comptes peuvent nécessiter la fourniture de photographies, de numéros de téléphone ou d'adresses électroniques au moment où ils sont créés. Les photos, numéros de téléphone, adresses électroniques et autres données qui sont personnelles ou attribuables aux enquêteurs ou à d'autres ne devraient jamais être utilisés.

Camouflage de l'utilisateur

107. Une identité virtuelle[120] est une fausse identité ou un faux profil en ligne qui peuvent être utilisés pour mener des activités d'enquête de façon sûre sur les plateformes de médias sociaux et d'autres plateformes ouvertes du Web dont les contenus ne sont accessibles que moyennant la connexion de l'utilisateur. Ces mesures de camouflage peuvent également inclure un compte virtuel ou encore une adresse électronique, une messagerie, une base de données, un produit ou une application qui utilisent une fausse identité en ligne plutôt que l'identité réelle de l'enquêteur ou de l'enquêtrice. Par souci de sécurité, les enquêteurs en sources ouvertes devraient se créer des identités virtuelles et les utiliser pour leurs activités d'enquête en ligne qui concernent

[118] Le retraçage consiste à rechercher l'origine de quelqu'un ou de quelque chose en remontant une piste d'informations ou une série de faits.

[119] Pour un examen des identités virtuelles, voir aussi les chapitres II.C, III.F, IV.A et IV.C ci-dessus.

[120] Toute utilisation d'une identité virtuelle doit concilier l'impératif de sécurité et le principe déontologique de transparence. Voir chap. II.C ci-dessus (Principes déontologiques).

des informations de sources ouvertes. Il s'agit de faire en sorte que l'acteur malveillant qui tenterait de suivre les activités en ligne d'un tel profil trouverait des informations cohérentes et convaincantes relatives à l'identité virtuelle, sans que ne lui soit révélé quoi que ce soit de réel concernant l'enquêteur ou l'enquêtrice, son entité ou le contenu ou l'objet de l'enquête. Ces dispositions sont également importantes pour toutes les personnes qui contribuent aux enquêtes. Les profils et les comptes virtuels, de même que les activités qui les utilisent, devraient être planifiés[121], les informations utilisées pour créer ces comptes devraient être conservées, et les activités menées avec ces comptes devraient être enregistrées pour qu'elles puissent être expliquées par la suite, si nécessaire, devant un tribunal, par exemple[122].

[121] Voir chap. V.C ci-dessous (Plan d'enquête en ligne).

[122] Voir chap. VI.D ci-dessous (Conservation).

V

PRÉPARATION

SOMMAIRE DU CHAPITRE

- La préparation et la planification stratégique de l'enquête sont essentielles à sa rigueur et à sa sécurité.
- La préparation comprend trois volets : a) l'évaluation des menaces et des risques et l'élaboration d'un plan d'atténuation de ces menaces et de ces risques ; b) l'état des lieux du paysage informationnel ; c) l'élaboration d'un plan d'enquête. Ces processus peuvent se chevaucher ou se répéter tout au long du cycle de vie de l'enquête.
- La préparation comprend un plan de gestion des incidences psychosociales négatives que pourrait avoir l'enquête, comme celles qui peuvent résulter de l'exposition à des documents choquants ou traumatisants.
- La préparation comprend un plan de gestion des informations collectées tout au long de leur cycle de vie, indiquant notamment à quel moment et dans quelles conditions elles doivent être supprimées, de quelle manière et dans quelles conditions elles peuvent être partagées, et qui peut y accéder.
- La préparation devrait comprendre une évaluation des logiciels et d'autres outils qui pourraient s'avérer utiles. Les enquêteurs devraient comprendre l'équilibre à réaliser entre les ressources commerciales, les ressources spécialement conçues et les ressources ouvertes

108. Les enquêteurs en sources ouvertes ne devraient entreprendre des activités d'enquête en ligne qu'après avoir effectué certains préparatifs. Ces préparatifs devraient comprendre une évaluation des menaces et des risques en ligne et une appréciation du paysage informationnel[123]. Les enquêteurs devraient alors élaborer des plans d'enquête en ligne, en y incluant les résultats de ces évaluations. L'une et l'autre de ces activités sont décrites ci-dessous.

109. Au niveau de l'organisation, il est important aussi d'adopter des politiques relatives à la conservation, la suppression, la consultation et la communication des données dès avant que les informations ne soient collectées et conservées, comme expliqué ci-dessous.

A. Évaluation des menaces et des risques

110. Le fait d'envisager les menaces possibles et d'adopter une stratégie de contrôle des risques – qu'ils soient d'ordre physique, numérique ou psychosocial – répond aux principes de sécurité et de déontologie. Une évaluation des menaces et des risques numériques devrait être réalisée dès le départ pour relever les menaces d'ordre général et ciblées qui pourraient se manifester par suite des activités en ligne, surtout s'agissant de se rendre sur des sites visés, d'assurer une surveillance continue de certaines sources ou d'extraire des données des plateformes de médias sociaux. L'évaluation devrait comporter des éléments de l'analyse des risques au sens traditionnel, comme le fait de répertorier tous les acteurs malveillants possibles, d'apprécier leurs intérêts et leurs capacités, de déterminer la mesure dans laquelle des attaques sont probables, de considérer les vulnérabilités et de mettre en place des mesures de protection pour les réduire au minimum. Il sera avantageux pour une telle évaluation de bénéficier de consultations avec des spécialistes de la sécurité, ou de contributions de la part de tels spécialistes, surtout s'ils sont experts dans le domaine de la cybersécurité[124]. L'évaluation devrait être revue périodiquement et mise à jour si nécessaire. D'autres évaluations pourraient être requises par rapport à certains types d'activités en ligne ou par suite de l'apparition d'éventuels nouveaux acteurs malveillants[125].

B. Appréciation du paysage numérique

111. Les enquêteurs en sources ouvertes devraient avoir une bonne compréhension de l'environnement numérique du dossier qui les occupe. Les types de moyens technologiques disponibles et utilisés, et leurs utilisateurs, sont des circonstances qui auront une incidence sur les types de données numériques disponibles. Il faut donc s'informer des plateformes en ligne, des services de communication, des plateformes de médias sociaux, des technologies mobiles et des applications mobiles les plus couramment utilisés dans la région géographique qui intéresse l'enquête. Dans le cas d'enquêtes portant sur des crimes de guerre, par exemple, les enquêteurs devront connaître les moyens de transport, les technologies de l'information et des communications et les médias numériques utilisés par toutes les parties au conflit armé, ainsi que par les tiers spectateurs ou par les autres témoins, pour savoir quels types d'informations sont les plus susceptibles d'être saisies et diffusées en ligne.

112. Les enquêteurs devraient examiner les catégories de personnes qui font usage ou qui ont l'usage de chacune de ces technologies dans la région géographique concernée. À cet égard, ils devraient savoir que les contenus numériques publics créés par des utilisateurs, y compris les publications sur les médias sociaux et les informations partagées par le truchement des plateformes de mise en réseau, peuvent ne pas rendre compte dans une mesure égale des violations commises à l'encontre de toutes les personnes et de tous les groupes. La raison en est que l'utilisation des technologies

[123] Voir annexe II (Modèle d'évaluation des menaces et des risques numériques) et annexe III (Modèle d'appréciation du paysage numérique).

[124] Pour des informations d'ordre général sur les menaces et les risques dans les enquêtes en sources ouvertes, voir chap. IV ci-dessus (Sécurité).

[125] Voir annexe II (Modèle d'évaluation des menaces et des risques numériques).

numériques peut varier en fonction de facteurs comme le genre[126], l'appartenance ethnique, la religion, les convictions, l'âge, la condition socioéconomique, l'appartenance à une minorité raciale, linguistique[127], ethnique ou religieuse, l'identité autochtone, le statut migratoire et la situation géographique[128]. Ces inégalités peuvent être le résultat d'un accès insuffisant aux appareils, aux installations ou aux ressources[129], qui fait que les personnes concernées n'ont pas l'occasion de créer ou de téléverser des informations en ligne sur les questions ou les violations qui les touchent. Il se peut aussi que les personnes mentionnées, parmi d'autres, n'ont pas bénéficié d'une éducation suffisante pour disposer des compétences techniques nécessaires. Par suite de discriminations croisées, certaines portions de la société peuvent être doublement invisibles en ligne. Ainsi, les femmes et les filles appartenant à un des groupes marginalisés précités pourraient-elles être encore moins représentées dans les informations de sources ouvertes que les membres masculins de leurs groupes. Les personnes affectées par ces facteurs risquent de ne pas être de celles qui produisent des contenus en ligne, ni de celles qui y figurent, ce qui tend à fausser les résultats des enquêtes.

113. En outre, les inégalités d'accès à la technologie que connaissent toutes les couches de la société sont de nature non seulement à fausser la représentation des personnes en ligne, mais aussi celle des types de violations, surtout lorsqu'il s'agit de contenus produits par de simples utilisateurs. Ainsi la femme qui partage l'usage d'un téléphone appartenant à un membre masculin de sa famille ou qui utilise le même compte en ligne que d'autres aura-t-elle tendance à ne pas aborder de questions sensibles, comme la violence sexuelle et fondée sur le genre, ou des questions touchant à la santé sexuelle et reproductive. À cela s'ajoute la possibilité que les contenus publiés par les utilisateurs des médias sociaux, notamment les photos et les vidéos, s'accommodent plus volontiers de certaines violations que d'autres. Ainsi la violence sexuelle et fondée sur le genre, qui peut se commettre en privé, se prête-t-elle moins à l'illustration en ligne que des faits tels que des expulsions, par exemple.

114. Bien que l'incidence de certains de ces facteurs puisse être atténuée en recherchant une pluralité de types d'informations en ligne, sans se cantonner aux contenus provenant des utilisateurs, il importe d'appliquer les mêmes considérations à l'analyse d'autres types d'informations de sources ouvertes. Dans le cas de données et de statistiques générées par des autorités, par exemple, les enquêteurs devraient toujours se demander si ces données portent bien sur toutes les parties et tous les aspects de la société[130]. L'attention peut se porter sur plusieurs questions et technologies clefs, selon ce qui est pertinent pour une enquête donnée compte tenu de sa portée géographique et temporelle. Les enquêteurs devraient prendre en compte le genre, l'âge, la géographie, les disparités socioéconomiques et d'autres informations démographiques utiles, le but de cette évaluation étant d'améliorer la compréhension que les enquêteurs ont des situations sous enquête, pour qu'ils soient en mesure de concevoir des stratégies d'enquête

[126] Par exemple, les femmes, les filles et les personnes lesbiennes, gays, bisexuelles, transgenres et intersexes peuvent ne pas avoir accès au téléphone portable de la famille, ou ne pas en être les détenteurs. Pour un examen plus approfondi de ce qui a été baptisé la « fracture numérique entre les genres », voir A/HRC/35/9. Voir aussi résolution 32/13 du Conseil des droits de l'homme, et Araba Sey et Nancy Hafkin, dir., *Taking Stock: Data and Evidence on Gender Equality in Digital Access, Skills, and Leadership* (Macao (Chine), EQUALS Global Partnership et Université des Nations Unies, 2019). Disponible à l'adresse www.itu.int/en/action/gender-equality/Documents/EQUALS%20Research%20Report%202019.pdf.

[127] Les personnes appartenant à des minorités linguistiques, par exemple, peuvent se trouver face à des obstacles lorsqu'elles essaient de se trouver une place en ligne, car les choses y sont habituellement menées dans la langue dominante. Certaines de ces minorités peuvent aussi avoir leur propre espace administré dans leur langue ou ouvert à celle-ci. Les enquêteurs pourraient avoir à effectuer des recherches dans les langues minoritaires (notamment dans les langues autochtones).

[128] Par exemple, la connectivité à Internet peut être moindre dans les zones rurales.

[129] Comme le fait de ne pas avoir à sa disposition de connexion Internet rapide ou le fait de ne pas avoir les moyens d'acquérir les appareils ou de s'acquitter des frais d'abonnement.

[130] Voir, à titre général, HCDH, Une approche des données fondée sur les droits de l'homme : Ne laisser personne de côté dans le programme de développement durable à l'horizon 2030 (Genève, 2018). Disponible à l'adresse www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData_FR.pdf.

en ligne efficaces et pour qu'ils soient tenus de faire face aux biais que pourraient présenter les informations disponibles en ligne. Comme toutes ces catégories ne valent pas nécessairement pour toutes les enquêtes, les enquêteurs devraient adapter l'état des lieux du paysage numérique à ce qui convient à une affaire précise[131]. Pour une liste complète des catégories d'informations qui peuvent être incluses dans une étude du paysage numérique, voir annexe III.

C. Plan d'enquête en ligne

115. Avant d'entamer une enquête en sources ouvertes, il est recommandé d'établir un plan d'enquête en ligne[132] qui couvre : a) la stratégie générale de l'enquête ; et b) les activités qui lui sont propres. Si ces activités s'inscrivent dans une enquête plus large qui fait appel à des techniques traditionnelles comme l'enregistrement de déclarations de témoins et la collecte d'éléments de preuve physiques, le plan d'enquête en ligne devrait s'intégrer dans le plan principal. Les enquêteurs en sources ouvertes devraient intégrer une perspective fondée sur le genre dans leur plan d'enquête, pour veiller à ce que leurs travaux portent sur toutes les questions touchant au genre et prennent en compte les différences d'accès aux moyens technologiques[133]. Le plan d'enquête en ligne devrait couvrir les sujets présentés ci-après.

1. Objectifs et activités prévues

116. Le plan devrait préciser les objectifs et les priorités de l'enquête en sources ouvertes, la stratégie envisagée pour les réaliser et le calendrier prévu à cette fin.

2. Stratégie de gestion des risques

117. Le plan devrait inclure les principales conclusions de l'évaluation des menaces et des risques numériques décrites ci-dessus, notamment en ce qui concerne la possibilité de cybermenaces, ainsi que la stratégie retenue pour contrôler les risques, dont les mesures prévues pour repérer les atteintes ou les attaques, y riposter et s'en remettre.

3. Cartographie des acteurs et des possibilités de coopération

118. Les enquêteurs en sources ouvertes pourraient répertorier les autres acteurs qui mènent des enquêtes similaires ou dont les travaux présentent des chevauchements avec ceux qu'eux-mêmes envisagent. Il s'agirait de déterminer les rapports utiles qui pourraient exister entre ces activités et d'envisager la possibilité de partenariats et de collaborations, notamment en repérant les archivistes numériques, les journalistes ou d'autres groupes d'individus qui conservent des contenus en ligne potentiellement utiles à l'enquête. Cette cartographie devrait aussi prendre en compte les biais et les limites qui pourraient caractériser d'autres acteurs et qui pourraient conduire à des constatations dégagées par des tiers ne rendant pas pleinement compte des complexités d'une situation donnée ou excluant certains groupes faute d'avoir tenu compte des biais inhérents à la sphère numérique, dont il a été question ci-dessus. Lorsque de tels partenariats sont conclus, il peut être utile d'établir un accord écrit de partage d'informations.

4. Ressources

119. Le plan devrait indiquer les ressources nécessaires pour mener à bien les activités prévues, y compris le personnel, la formation, les outils et le matériel. L'évaluation des besoins en personnel peut porter sur le nombre de personnes que l'équipe doit compter pour accomplir les tâches, les compétences que doivent avoir ces personnes, les caractéristiques d'inclusivité et de diversité que doit présenter l'équipe, ainsi qu'une évaluation des besoins supplémentaires en formation. Le plan peut comprendre une évaluation des besoins infrastructurels, dont les matériels et les logiciels, ainsi que de la charge financière

[131] Pour le modèle, voir annexe III.

[132] Pour le modèle du plan d'enquête en ligne, voir annexe I.

[133] Pour de plus amples orientations concernant l'intégration d'une perspective fondée sur le genre, voir *L'intégration d'une perspective fondée sur le genre dans les enquêtes sur les droits de l'homme : Guide pratique* (New York et Genève, Nations Unies, 2019).

que représentera la conservation à long terme des éléments recueillis. Le plan devrait aussi prévoir l'allocation de ressources propres pour veiller, en tenant compte des questions de genre, au bien-être psychosocial des enquêteurs, en particulier lorsque des contenus choquants interviennent dans l'enquête ou lorsque des enquêteurs ou des tiers courent un risque particulier de représailles en cas de divulgation de leur identité ou d'aspects de leur vie privée[134].

5. Rôles et responsabilités

120. Lorsque le travail s'accomplit en équipe ou avec des partenaires externes, les rôles et responsabilités des enquêteurs en sources ouvertes devraient être bien définis, compte tenu de la nécessité de coordonner le travail, notamment pour éviter le chevauchement des activités et de la collecte des données. Cette partie du plan devrait en outre indiquer quelles compétences spéciales seront requises pour mener l'enquête, et préciser s'il y aura lieu pour les enquêteurs de consulter ou d'engager un expert ou une experte lorsqu'un domaine de compétence n'est pas représenté au sein de l'équipe. Parmi ces compétences spéciales pourront figurer la criminalistique numérique, l'analyse des images satellites et la science des données. Dans certains domaines de compétence, les devants pourraient être pris afin d'identifier des spécialistes présentant une diversité de genres et d'autres caractéristiques, afin d'assurer l'inclusivité et la diversité de l'équipe d'enquête et de ses analyses.

6. Consignation

121. Les activités des enquêtes de sources ouvertes devraient être consignées de sorte à permettre leur gestion efficace et le respect du principe de responsabilité. Dans le cas d'une procédure judiciaire, les enquêteurs devraient pouvoir, sur la base des faits d'enquête ainsi répertoriés, démontrer que les éléments de preuve collectés sont pertinents et probants, rapporter ce qui a été fait, ou ce qui n'a pas été fait, selon les cas, dans le cadre du travail en ligne, et expliquer pourquoi il a été procédé de la sorte. Que l'enquêteur ou l'enquêtrice agisse indépendamment ou selon les directives d'un supérieur ou d'une supérieure, le système devrait comporter un mécanisme qui génère des tâches à accomplir dans le cadre des activités d'enquête, y compris des tâches en ligne, comme des demandes de renseignements sur telle ou telle personne, ou d'autres recherches. Les résultats de ces tâches, notamment les rapports, devraient renvoyer aux méthodes et techniques utilisées. Aux fins de l'établissement des rapports d'enquête, les informations opérationnelles dont la confidentialité doit être maintenue pour protéger les sources et les méthodes d'un enquêteur ou d'une enquêtrice devraient être séparées des résultats de l'enquête appelés à être présentés dans le cadre d'une procédure judiciaire.

122. Le plan d'enquête en ligne devrait être revu régulièrement et modifié si nécessaire. Son modèle est présenté à l'annexe I.

D. Plan de résilience et autosoins

123. S'il est vrai que les enquêteurs en sources ouvertes peuvent ne pas avoir à mener des entretiens en tête à tête ou à se rendre sur les lieux de crimes, les particularités de la recherche numérique sont telles que ceux qui la pratiquent sont amenés à visionner, à recueillir et à analyser d'importantes quantités d'informations numériques susceptibles de choquer et de traumatiser au point de provoquer des traumatismes secondaires et d'autres problèmes. Les enquêteurs en sources ouvertes devraient connaître les méthodes d'autosoins (self-care) qui permettent de

[134] À titre d'exemple, les enquêteurs peuvent faire l'objet de propos haineux ou de harcèlement en ligne et ces attaques peuvent viser le genre (ainsi les femmes et les personnes lesbiennes, gays, bisexuelles, transgenres, queers et intersexes qui mènent des enquêtes en ligne sont-elles plus exposées que la moyenne aux discours de haine, au « doxing », aux menaces de viol et à d'autres menaces violentes à caractère sexuel ou fondées sur le genre). Voir, par exemple, Amnesty International, « Toxic Twitter – a toxic place for women ». Disponible à l'adresse www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/.

maintenir son équilibre[135], et celles et ceux qui dirigent les enquêtes devraient faire régner dans leurs équipes l'encouragement à prendre soin de soi-même et la sensibilité aux questions de genre et de culture. Cette ambiance de travail devrait être instaurée dès les préparatifs de l'enquête, par la mise au point d'un plan visant à encourager la résilience et à atténuer les effets psychologiques négatifs que pourrait avoir une enquête, sachant que ces effets peuvent varier selon le genre, la culture et l'âge. Un tel plan est essentiel non seulement sur le plan moral, pour promouvoir le respect des droits humains de chaque membre de l'équipe d'enquête, mais aussi pour assurer une sécurité physique et numérique maximale. En effet, même avec la formation voulue, un individu stressé peut représenter une vulnérabilité pour la sécurité de son équipe, celle des informations et la qualité du travail. Du temps et des ressources devraient être spécialement consacrés à la bonne exécution du plan, tout particulièrement lorsqu'il est prévu que les enquêteurs prennent connaissance d'une grande quantité d'images choquantes, notamment des contenus violents ou troublants. Les stratégies visant à atténuer les effets négatifs potentiels de l'exposition à des contenus choquants sont diverses, mais tendent à se classer en trois catégories : prise de conscience individuelle, techniques de réduction de l'exposition et soutien de proximité.

124. Tout d'abord, les enquêteurs devraient avoir conscience de leurs comportements habituels ainsi que de ceux des autres membres de leur équipe, notamment des habitudes de travail, de détente, de sommeil et d'alimentation, de sorte que tout écart puisse être détecté et donner lieu à la suite voulue. Le fait d'avoir pour règle de travailler en binômes peut faciliter cette détection, la personne affectée n'étant pas toujours capable ou désireuse de reconnaître les modifications de son propre comportement que d'autres relèveront plus facilement. Les membres de l'équipe devraient faire preuve de sensibilité et de respect à l'égard des différentes façons de réagir aux contenus susceptibles de choquer ou de provoquer de fortes émotions, et savoir que ces réactions peuvent varier selon les individus, les genres et les groupes culturels, de même qu'au fil du temps pour une même personne, en fonction du stress et d'autres facteurs situationnels qui agissent sur elle. Les enquêteurs devraient également reconnaître que, loin d'être le signe d'une faiblesse de caractère, réagir émotionnellement à un contenu choquant est souvent tout à fait normal, et même la manifestation d'une attitude saine, voire forte.

125. Ensuite, il faudrait adopter des techniques pour réduire l'exposition à des contenus préjudiciables. Les plus communes à cet égard consistent notamment à : couper le son lorsqu'on regarde pour la première fois une séquence qui risque de choquer ou lorsque le son n'est pas nécessaire pour la tâche analytique en cours, car la bande-son peut avoir une forte charge émotive ; réduire autant que faire se peut la taille des écrans de visionnage ; couvrir les aspects choquants d'une séquence lorsqu'il est simplement question d'analyser le contexte dans lequel un acte a été commis, et non l'acte lui-même ; signaler la présence de tout contenu choquant dans un ensemble de données, pour que personne n'y soit exposé sans avoir été prévenu ; se prévenir les uns les autres lorsque sont envoyés des contenus choquants, pour réduire l'effet de surprise ; travailler en binômes ; éviter de travailler lorsqu'on est isolé ou tard le soir ; s'accorder régulièrement des pauses, selon ce qui est nécessaire.

126. Enfin, les individus et les organisations devraient encourager parmi les membres de l'équipe un esprit de communauté qui peut avoir un effet protecteur, à l'image de l'esprit de camaraderie qui peut exister parmi les enquêteurs lorsqu'ils travaillent sur le terrain. Ce résultat peut être obtenu par les mesures suivantes : la tenue régulière de réunions de bilan, lesquelles peuvent réduire l'isolement et aider les enquêteurs à mieux saisir les effets positifs de leur travail ; les sorties en équipe, notamment pour célébrer des réalisations importances dans les enquêtes ; la formation de l'équipe aux stratégies de résilience. Les mesures tendant à accroître la résilience peuvent s'avérer particulièrement efficaces lorsqu'elles se conçoivent aux niveaux

[135] Pour un examen plus approfondi de l'importance des autosoins pour celles et ceux qui travaillent dans le domaine des enquêtes relatives aux droits humains, voir OHCHR, *Manual on Human Rights Monitoring* (Genève, 2011), chap. 12 (Trauma and self-care), p. 20 à 39. Disponible à l'adresse www.ohchr.org/Documents/Publications/Chapter12-MHRM.pdf.

individuel, culturel et structurel, notamment en habilitant les individus à réfléchir de manière critique à leurs besoins psychosociaux lorsqu'ils se consacrent à une enquête, et en favorisant un environnement dans lequel les aspects psychosociaux du travail sont pris au sérieux, les pratiques de soutien sont implicitement et explicitement encouragées, et une large place est accordée à l'inclusivité comme à la diversité.

E. Politiques et outils relatifs aux données

127. L'ouverture d'une enquête devrait donner lieu à l'élaboration et à l'application de politiques concernant le traitement, la conservation et la destruction des données. Les organisations devraient, le cas échéant, élaborer des règles relatives à la conservation et à la suppression des informations (politiques de conservation et de suppression), de même que des règles relatives à l'accès aux informations (par des parties internes) et au partage des informations (avec des parties externes). Elles pourraient également avoir intérêt à se doter de règles pour la création et l'utilisation des identités virtuelles, ainsi que pour l'accès aux logiciels approuvés et aux outils désignés.

1. Politiques relatives aux données

a) Conservation des données

128. Les politiques de conservation des données sont importantes pour se conformer aux nombreuses lois régissant la protection des données et aux nombreuses réglementations encadrant la conservation des données. Dans certains cas, il est prévu une période minimum pendant laquelle les données doivent être conservées, dans d'autres, il est question d'une période maximum pendant laquelle elles peuvent être conservées. Les politiques devraient énoncer les méthodes de stockage des données permanentes et de gestion des archives dans le but de respecter les exigences légales et professionnelles en matière d'archivage des données. Les politiques de conservation des données mettent en balance les préoccupations relatives à la législation et à la vie privée, d'une part, et les préoccupations économiques et liées au besoin d'en connaître, d'autre part, pour déterminer les temps de conservation, les règles d'archivage, les formats de données et les modalités autorisées de stockage, d'accès et de chiffrement[136]. À l'évidence les règles en vigueur seront nécessaires pour l'établissement de ces politiques.

b) Suppression des données

129. Le fait de supprimer des parties d'un ensemble de données en l'absence de politiques régissant clairement la suppression et la conservation des données, ainsi que de registres indiquant ce qui a été supprimé, par qui et quand – et à quelles fins – peut poser de graves problèmes, tout particulièrement lorsque les informations sont susceptibles d'être présentées devant un tribunal. Les enquêteurs devraient suivre les règlements applicables lorsqu'il s'agit de supprimer des données numériques, et être conscients que le choix de telle méthode plutôt qu'une autre pour ce faire peut soulever des questions juridiques.

c) Accès aux données

130. Les organisations qui collectent et traitent des données, et à plus forte raison lorsque les données sont sensibles, devraient avoir une politique clairement établie pour déterminer qui peut accéder aux divers types de données, et leurs bases de données et autres systèmes concernés devraient être réglés pour refléter cette politique.

d) Partage des données

131. Les organisations pourraient envisager d'élaborer une politique relative au partage des données avec les acteurs extérieurs, et si elles travaillent avec des partenaires extérieurs, elles devraient passer avec eux des mémorandums d'accord ou des contrats pour veiller à ce qu'ils respectent cette politique.

[136] Yvonne Ng, « How to preserve open source information effectively », dans *Digital Witness, Using Open Source Information for Human Rights Investigation, Documentation and Accountability*, Sam Dubberley, Alexa Koenig et Daragh Murray, dir. (Oxford, Oxford University Press, 2020), p. 143 à 164.

2. Gestion de l'information

132. Avant d'entreprendre des enquêtes en sources ouvertes, et plus particulièrement de collecter et de conserver des éléments numériques, les enquêteurs, les équipes et les organisations devraient se doter d'un système de gestion de l'information. Il existe un éventail de systèmes possibles. Le Protocole n'en préconise pas une en particulier, mais présente ci-après les principales fonctionnalités qui peuvent être utiles – et qui, dans certains contextes, peuvent être requis – aux fins du processus d'enquête. Il faudrait en outre, comme expliqué au chapitre IV, que soient mis en place une infrastructure et des protocoles de sécurité.

a) Système de gestion des enquêtes

133. Un système de gestion des enquêtes est un système qui répertorie les activités menées aux fins de l'enquête. Toutes les organisations qui enquêtent ne disposent pas de tels systèmes, mais ils sont hautement recommandés, surtout pour les organisations ou les équipes de plus grande taille. Ils peuvent être utilisés pour assigner les tâches et rendre compte des activités, afin que le processus soit structuré et le plus efficace possible, étant donné qu'ils peuvent contribuer à réduire le chevauchement des travaux.

b) Systèmes de gestion de l'information et des éléments de preuve

134. Les systèmes de gestion de l'information sont utilisés pour stocker les données collectées dans le cadre des enquêtes. Ils doivent pouvoir assurer deux fonctions distinctes : a) le suivi de la collecte et du traitement des éléments ; b) la séparation des éléments qui pourraient contribuer à la preuve.

3. Infrastructure – considérations relatives à la logistique et à la sécurité

135. Qu'il s'agisse de concevoir l'infrastructure destinée à une organisation qui mène des enquêtes en sources ouvertes ou de décider quels outils utiliser en tant qu'enquêteur ou qu'enquêtrice indépendant(e), plusieurs considérations importantes concernant la logistique et la sécurité entrent en jeu. Il y a généralement trois façons d'envisager l'acquisition de systèmes : a) concevoir ses propres systèmes et outils ; b) utiliser des outils et des logiciels open source ou libres disponibles sur Internet ; c) acheter des produits commerciaux à des tiers. Chacune de ces démarches a ses avantages et ses inconvénients, et les résultats obtenus dépendront des circonstances et du contexte particuliers dans lesquels les enquêteurs travaillent. Comme indiqué précédemment, le Protocole n'entend pas conseiller une démarche plutôt qu'une autre ; il présente ci-après les avantages et les inconvénients de chaque possibilité, ainsi que les facteurs à prendre en compte pour décider quels produits utiliser.

a) Produits commerciaux

136. Les produits commerciaux ont pour avantage que l'entreprise privée qui les fournit pourrait disposer d'une meilleure infrastructure de sécurité et apporter un appui technique continu et constant. Les produits commerciaux ont toutefois le désavantage évident du coût. De plus, le fait de traiter avec une entité extérieure et de dépendre d'elle peut s'avérer problématique pour des organisations qui s'efforcent de préserver la confidentialité de leurs enquêtes. De nombreux produits commerciaux utilisent des codes sources fermés pour protéger leur propriété intellectuelle. Les produits commerciaux peuvent également susciter des préoccupations quant à la propriété, la transférabilité et l'exportation les données, ainsi qu'en matière d'interopérabilité. À cela s'ajoute que les entreprises peuvent céder aux pressions des autorités publiques qui demandent à accéder aux informations privées. Une préoccupation majeure suscitée par la solution commerciale réside dans le fait que même si les entreprises concernées ont des équipes de sécurité pour protéger leurs produits et leurs utilisateurs, les utilisateurs doivent pouvoir compter sur le fait que les fournisseurs auront bien conçu leurs systèmes, qu'ils en assureront la bonne maintenance et qu'il n'y aura pas de coûts cachés à un stade ultérieur.

b) Outils spécialement conçus ou adaptés

137. La conception de son propre outil de A à Z, ou l'adaptation d'un outil existant, ont pour avantage que les organisations ou les enquêteurs gardent le contrôle du système tout

entier et de leurs données et qu'ils peuvent de ce fait éviter l'interaction avec d'autres parties. Les systèmes spécialement conçus peuvent aussi s'intégrer plus aisément avec d'autres systèmes sur mesure. Du côté des inconvénients, il y a le temps, le coût et les compétences spécialisées que demandent la construction et la prise en charge de tels systèmes, et qui constitueront des obstacles pour la plupart des organisations. En outre, le fait de travailler avec un système fermé qui ne compte que peu de bêta testeurs et d'utilisateurs peut rendre difficile la détection de ses vulnérabilités et l'obtention de retours d'expérience suffisants pour en optimiser le fonctionnement.

c) Outils open source et libres

138. Les outils open source sont des outils dont les codes sources ont été ouvertement publiés par les concepteurs de sorte que tout un chacun puisse les utiliser et les modifier librement. Certains produits commerciaux existent avec des codes ouverts et certains outils libres sont disponibles avec des codes fermés, mais ce sont des exceptions. Le plus souvent, les outils open source sont libres. Pour les organisations de plus petite taille dont les budgets sont limités, de même que pour les plus grandes dont les procédures d'acquisition de produits payants sont fastidieuses, la solution des outils libres peut avoir toute son importance. Cela étant, les outils mis gratuitement à la disposition des utilisateurs peuvent générer des bénéfices d'autres façons, notamment par la vente de données et d'analyses de données relatives aux utilisateurs, ce qui soulève des questions de sécurité et de vie privée. Par ailleurs, l'utilisation de ces outils nécessite des recherches préalables afin de déterminer par qui ils ont été créés, s'ils ont été vérifiés de façon indépendante et s'ils sont viables. Ce sont autant de points qui pourraient compromettre la crédibilité d'une enquête, et qui pourraient s'avérer particulièrement problématiques dans un contexte judiciaire, lorsqu'une affaire est portée devant les tribunaux et que la partie adverse conteste l'outil utilisé. En outre, ces solutions logicielles nécessitent la mise en place d'un plan de secours assorti d'un système de migration et de sauvegarde des données aux cas où elles deviendraient obsolètes ou leurs concepteurs indisponibles. Si l'attraction des outils open source pour les organisations peut venir en partie du fait que d'autres groupes attachés aux mêmes principes en font usage, les enquêteurs n'en doivent pas moins faire procéder à une évaluation indépendante complète de leur façon de travailler et des implications que leur utilisation pourrait avoir dans un contexte donné.

139. Pour faire leur choix entre un système spécialement conçu, l'utilisation d'un logiciel en essai libre ou open source, ou l'achat d'un produit, les enquêteurs devraient suivre les précautions qui s'imposent, telles qu'elles sont énoncées à l'annexe V.

VI

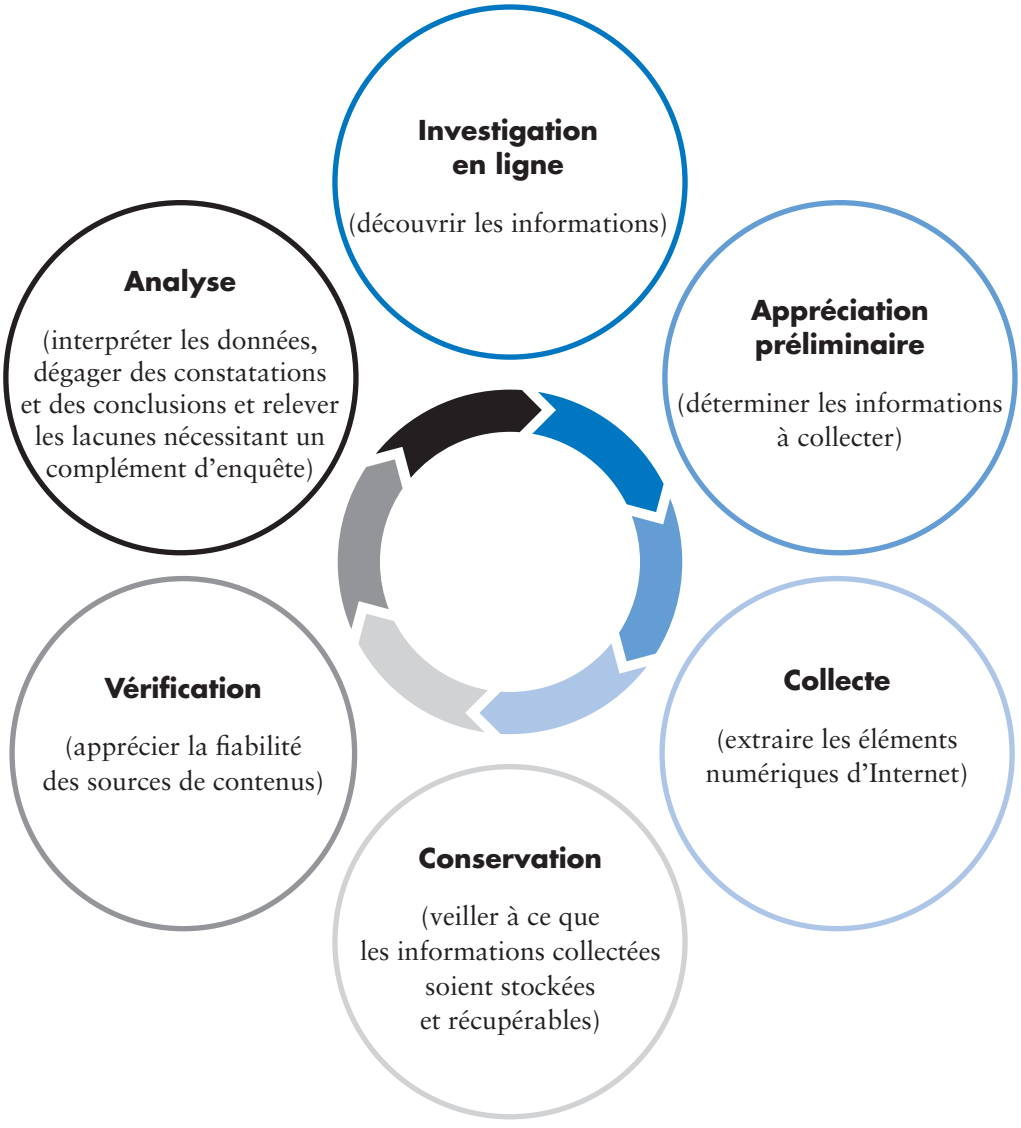
TÂCHES DE L'ENQUÊTE

SOMMAIRE DU CHAPITRE

- Les tâches de l'enquête s'articulent en six phases principales : a) les investigations en ligne ; b) l'appréciation initiale ; c) la collecte ; d) la conservation ; e) la vérification ; f) l'analyse. Ensemble, ces phases constituent un cycle qui peut être répété de nombreuses fois au cours d'une enquête, au fur et à mesure que de nouvelles informations conduisent à de nouvelles pistes d'investigation.
- Les enquêteurs devraient consigner les activités qu'ils entreprennent pendant chacune de ces phases. Cela rendra leurs enquêtes plus compréhensibles et transparentes, notamment pour ce qui a trait aux chaînes de contrôle, et plus efficientes et efficaces, notamment pour ce qui a trait à l'impératif de complétude et à la communication parmi les membres de l'équipe.

140. Les enquêtes en sources ouvertes requièrent une observation attentive et des recherches systématiques afin d'établir les faits dans un environnement numérique complexe et dynamique. Les enquêteurs en sources ouvertes doivent poser un regard critique sur les contenus en ligne pour décider s'ils peuvent être retenus et pour déterminer de quelles manières ils auraient pu être déformés ou manipulés. Ils devraient aussi structurer leurs recherches sur Internet en tenant compte des biais algorithmiques, de la disponibilité inégale des informations de sources ouvertes selon qu'elles concernent tel ou tel groupe, et de la nature dynamique des informations en ligne. Chaque acte allégué doit être rigoureusement examiné. Le présent chapitre présente une approche structurée de l'enquête en sources ouvertes. La figure ci-après illustre le cycle de l'enquête en source ouverte. Il importe de retenir que les enquêtes en sources ouvertes ne sont que rarement linéaires et qu'elle requièrent souvent la répétition de ce processus, conformément à la nature cyclique de la constitution d'un dossier. Cela étant, il peut aussi y avoir des raisons valables de s'écarter de cette séquence.

Cycle de l'enquête en sources ouvertes



A. Investigations en ligne

141. Les investigations en ligne comprennent deux tâches principales : a) les recherches, c'est-à-dire la découverte d'informations et de sources d'information au moyen de méthodes générales et spécialisées ; b) la surveillance, c'est-à-dire la découverte d'informations par l'examen constant et persistant d'un ensemble de sources déterminées.

1. Recherches

142. Les recherches en ligne consistent à accomplir un certain nombre de tâches destinées à découvrir de nouvelles informations relatives à un objectif défini ou à une question posée. Les activités de recherche devraient être structurées et systématiques, et notamment s'entreprendre sur la base d'une question claire et de paramètres de recherche définis, ainsi que de mots clefs et d'opérateurs[137]. Comme différents moteurs de recherche, outils de recherche, termes de recherche et opérateurs donneront des résultats différents, les enquêteurs devront faire preuve d'une certaine créativité et d'une certaine ténacité pour suivre les diverses voies qui pourraient les mener aux informations qui les intéressent. Outre les moteurs de recherche utilisés pour trouver les informations qui se trouvent sur des sites Web indexés, des recherches structurées peuvent également être effectuées sur les plateformes de médias sociaux et dans les bases de données. Comme il est nécessaire de varier et de diversifier les moyens de recherche et de les adapter selon les enquêtes, les enquêteurs devraient prendre soin de consigner les façons dont ils procèdent pour qu'elles puissent être expliquées dans la partie méthodologique des rapports d'enquête ou devant les tribunaux. Si la consignation peut être rétroactive, en ce sens qu'elle ne doit pas nécessairement avoir lieu en parallèle avec la recherche elle-même, elle devrait toujours avoir lieu aussi près que possible de la date des activités qu'elle répertorie. Dans le cas des recherches structurées, les informations suivantes devraient être consignées :

a) L'objectif et les questions de la recherche : énoncer la ou les questions auxquelles la recherche en ligne entend répondre, en gardant à l'esprit le principe d'objectivité établi ci-dessus ;

b) Les faits, les hypothèses et les inconnues : partir d'un point où les faits sont connus, s'ils ont été établis. Il pourrait aussi s'avérer utile de prendre comme point de départ des indices ou des hypothèses logiques, même s'il s'agit d'éléments qui n'ont pas encore été vérifiés. Il est cependant essentiel d'enregistrer toutes les hypothèses comme telles. Il peut aussi être avantageux de formuler les lacunes dans la connaissance du dossier ou d'autres « inconnues » dès le début de l'enquête. Délimiter ces catégories d'informations, en précisant les termes de recherche et les bases sur lesquels elles sont fondées, contribuera à éviter les résultats biaisés ou déformés ;

c) Termes de recherche et mots clefs : afin de cibler leurs recherches, les enquêteurs devraient établir des listes de mots clefs, conformes au principe d'objectivité, basés sur le ou les raisonnements associés au dossier. Idéalement, ils utiliseront des mots clefs dans toutes les langues et toutes les écritures concernées, et seront attentifs au fait que leurs recherches pourraient produire des résultats trop étendus ou trop limités. Malgré ce qui différencie les affaires, il est des rubriques générales qui devraient à chaque fois être incorporées dans les listes de mots clefs, tels que les lieux, les personnes, les organisations, les dates et les mots-dièse ou hashtags concernés. Il pourrait également être utile de relever les éléments susceptibles d'être à charge ou à décharge dans le cadre de chaque enquête ;

d) Recherches et moteurs de recherche : les enquêteurs devraient suivre leurs recherches et consigner les chemins qu'ils ont parcourus pour arriver aux éléments pertinents, y compris les termes de recherche, les opérateurs et les moteurs de recherche qu'ils ont utilisés à cette fin.

[137] Les opérateurs booléens sont des mots simples, tels que « et » (and), « ou » (or) et « sauf » (not), qui peuvent s'utiliser pour « combiner ou exclure des mots clefs dans le cadre d'une recherche, afin d'obtenir des résultats plus précis et utiles ». Voir Alliant International University Library, « What is a Boolean operator? ». Disponible à l'adresse https://library.alliant.edu/screens/boolean.pdf.

Il n'est toutefois pas nécessaire de consigner tous les résultats des recherches, ce serait trop fastidieux et n'aurait que peu de valeur probante.

2. Surveillance

143. La surveillance consiste à suivre une source d'information établie, sur un sujet donné, par exemple, pendant un certain temps. Il s'agit d'observer le contenu changeant d'une source constante. La surveillance en ligne devrait être une activité structurée, fondée sur une liste de sources connues et précédemment évaluées, qui peuvent être des sites Web ou des comptes de médias sociaux, ainsi que sur des requêtes de recherche qui sont lancées en continu contre des cibles définies. Voir, par exemple, les sources suivantes :

a) Sites Web et comptes de médias sociaux : les enquêteurs devraient tenir des listes de sites et de profils à suivre. Ces listes de travail devraient inclure une justification de la surveillance de chaque source, le nom de la personne qui en est responsable, le nom de la ou des personnes qui l'effectuent, et sa fréquence ;

b) Mots-dièse (hashtags) et mots clefs : les enquêteurs devraient également tenir, en les actualisant régulièrement, une liste de travail des mots-dièse et des mots clefs qui sont surveillés ;

c) Automatisation : la surveillance peut se faire au moyen d'outils automatisés, ceux-ci pouvant, par exemple, effectuer une recherche périodique sur des sites donnés ou selon certains paramètres. L'utilisation de tels outils, leur nom, leur version et les informations sur la base desquelles ils effectuent leurs recherches devraient toujours être enregistrés.

3. Biais

144. Lorsqu'ils effectuent des recherches structurées ou mènent des activités de surveillance, les enquêteurs en sources ouvertes doivent toujours être attentifs aux possibilités de biais, qu'il s'agisse de leur propre biais cognitif ou du biais inhérent aux informations disponibles en ligne. Si un enquêteur ou une enquêtrice cherche des informations relatives au viol, par exemple, la majorité des informations fournies ou des questions abordées en ligne porteront probablement sur les viols commis hors de la sphère maritale sur la personne de femmes en âge de procréer. Les résultats des recherches en ligne pourraient ainsi ne pas rendre suffisamment compte de formes de viols de moindre visibilité, telles que les violences sexuelles à l'encontre des hommes et des garçons, des personnes lesbiennes, gays, bisexuelles, transgenres et intersexes, et des femmes plus âgées, ainsi que le viol conjugal.

145. Les enquêtes sur les violences provoquées par les discours de haine sont un autre exemple, dès lors que les discours en question comprennent souvent des expressions codées et des symboles qui ne sont pas aisément détectables par les enquêteurs ou les machines. Lorsque les enquêteurs n'appartiennent pas aux communautés visées, en particulier, ils peuvent ne pas être conscients des usages culturels et contextuels des termes et symboles utilisés pour inciter à la haine ou à la violence. Cette situation se trouve encore compliquée par le fait que les discours de haine en ligne sont souvent conçus pour échapper à la surveillance des machines comme des humains et éviter ainsi d'être supprimés des plateformes, alors qu'ils ont bien pour but d'inciter à la violence ou à la discrimination contre telle ou telle population. Pour rendre moins difficile la détection des cas d'incitation à la discrimination, à l'hostilité ou à la violence, les enquêteurs devraient procéder à un examen axé sur les droits humains, tel que celui prévu par le Plan d'action de Rabat sur l'interdiction de l'appel à la haine nationale, raciale ou religieuse qui constitue une incitation à la discrimination, à l'hostilité ou à la violence[138].

146. En définitive, la meilleure façon pour les enquêteurs de contrer les biais de la machine et de l'humain est d'être conscients que ces biais peuvent exister, de reconnaître les risques qu'ils représentent et de prendre, lorsque c'est possible, des mesures actives

[138] Voir HCDH, « La liberté d'expression contre l'incitation à la haine : le HCDH et le Plan d'action de Rabat ». Disponible à l'adresse https://www.ohchr.org/fr/freedom-of-expression.

pour les contrecarrer, en étudiant les termes et les symboles qui se rapportent à un certain contexte ou à un ensemble de crimes ou de faits, et en élargissant l'investigation en ligne. Dans les cas de violence sexuelle ou de violence fondée sur le genre, ainsi que pour toutes autres infractions dont les survivants sont stigmatisés et dont on parle en langage codé, les enquêteurs devraient consulter des spécialistes qui pourraient les aider à reconnaître et à faire connaître les expressions codées et les pratiques de communication auxquelles ces survivants et les auteurs des actes en question ont souvent recours pour communiquer dans les espaces en ligne[139].

B. Appréciation préliminaire

147. Avant de collecter du contenu sur Internet, les enquêteurs en sources ouvertes devraient soumettre tout élément repéré à une appréciation préliminaire afin d'éviter toute collecte excessive, de se conformer aux principes de la minimisation des données et du ciblage des enquêtes et d'éviter que la collecte envisagée ne porte atteinte au droit à la vie privée. Les enquêteurs en sources ouvertes devraient considérer les facteurs suivants pour déterminer si un élément numérique devrait être extrait d'Internet.

1. Pertinence

148. Les enquêteurs en sources ouvertes devraient déterminer si l'élément numérique considéré se rapporte à première vue à leur enquête. La pertinence de tout élément sera fonction de son contenu et de sa source, ainsi que des objectifs de l'enquête et de ce qui est connu de la situation sous enquête. Comme il peut être difficile de savoir ce qui est utile alors que l'enquête n'en est qu'à ses débuts, les enquêteurs peuvent se laisser tenter par une collecte excessive à ce stade. Il n'en reste pas moins qu'ils devraient être en mesure de dire pourquoi ils estiment que tel ou tel élément pourrait être utile, et qu'ils devraient consigner cette appréciation (par exemple, au moyen d'un système de marquage ou de stockage simple et convivial qui relie les informations collectées à des aspects de l'enquête comme un lieu, une date, certains faits, une personne ou un type d'infraction).

2. Fiabilité

149. Les enquêteurs en sources ouvertes devraient déterminer si les informations fournies ou les prétentions avancées dans un contenu numérique sont de prime abord fiables, et pour cela examiner et apprécier le contenu et ses éléments contextuels. Il s'agira notamment de vérifier les métadonnées qui y sont intégrées, les informations qui y sont liées et la source qui l'a produit[140]. Il faudrait notamment essayer d'identifier la source originelle de l'élément, ce qui peut amener à rechercher l'origine en ligne des données, leur téléverseur et leur auteur.

3. Suppression

150. Les enquêteurs en sources ouvertes devraient apprécier si un élément numérique est susceptible d'être supprimé d'Internet ou s'il risque de ne plus être public. Lorsque la suppression d'un contenu est probable, la version la plus fiable qui en soit connue devrait être collectée, même si des vérifications et des investigations concernant des versions antérieures ou meilleures sont encore en cours. La probabilité d'une suppression de contenu peut être appréciée au regard de plusieurs facteurs, parmi lesquels l'identité de la source, l'emplacement du contenu et sa compatibilité avec les conditions de service du prestataire de services. Ainsi le contenu choquant ou offensant qui pourrait avoir une grande valeur probante pour l'établissement d'un crime ou d'une violation comptera-t-il parmi les principaux candidats à la suppression.

4. Sécurité

151. Les enquêteurs en sources ouvertes devraient déterminer si la collecte d'un élément numérique est sûre ou si des précautions supplémentaires pourraient et devraient

[139] Voir, par exemple, Koenig et Egan, « Hiding in plain site: using online open source information to investigate sexual violence and gender-based crimes ».

[140] Voir chap. VI.E ci-dessous (Vérification).

être prises. Les préoccupations de cet ordre sont plus probables en présence de sites Web qui pourraient contenir des éléments altérés capables d'endommager le système interne.

5. Obligations subséquentes

152. Les enquêteurs en ligne devraient déterminer quelles obligations pourraient s'imposer à eux lorsqu'ils détiennent un élément numérique, notamment l'obligation de le conserver de façon sûre pour respecter les lois relatives à la protection des données[141].

C. Collecte

153. La collecte est l'acte de prendre possession d'informations en ligne au moyen d'une capture d'écran, d'une conversion sous format PDF, d'un téléchargement de criminalistique ou d'une autre forme de saisie. Une fois que le contenu numérique a été repéré, jugé en rapport avec l'enquête, est pertinent et fiable à première vue au regard de l'objectif de celle-ci, l'enquêteur ou l'enquêtrice doit déterminer la bonne méthode de collecte. Les méthodes de collecte peuvent varier selon que le contenu en ligne pourrait servir de preuve dans une procédure judiciaire, sera utilisé à des fins décisionnelles ou qu'il ne contribuera qu'à un travail interne. Lorsqu'il s'agit simplement d'un travail interne, une capture d'écran ou une conversion sous format PDF pourraient suffire, tandis que le contenu qui a une valeur probante pourrait nécessiter une méthode de capture plus rigoureuse et sûre (consistant notamment à lui associer une empreinte numérique ou valeur de hachage – voir ci-dessous).

154. La collecte de contenu en ligne peut s'effectuer manuellement, selon une procédure établie, ou automatiquement au moyen de divers outils ou scripts. Quel que soit le procédé retenu, les informations répertoriées ci-dessous devraient idéalement être saisies au point de collecte. Ces informations pourraient s'avérer utiles pour établir l'authenticité d'un élément numérique, chose particulièrement importante s'il doit être produit en preuve dans une procédure judiciaire, et d'autant plus importante si l'auteur ou le créateur n'est pas identifié, localisé ou disponible aux fins d'une déposition. Les enquêteurs en ligne devraient collecter les contenus en ligne dans leur état d'origine ou dans un état aussi proche que possible de son format originel. Toute modification, transformation ou conversion causée par le processus de collecte devrait être consignée.

155. Ce paragraphe fournit des orientations concernant les informations à collecter et les modalités de collecte. Plusieurs outils peuvent contribuer à la saisie des informations répertoriées ci-dessous, qui peut aussi se réaliser manuellement. Bien qu'il soit de bonne pratique de recueillir toutes les informations mentionnées, les trois premiers éléments (le localisateur uniforme de ressources ou URL, le code source en langage de balisage hypertexte ou code source HTML, et la capture pleine page) constituent un minimum pour fournir des éléments de preuve en justice. Ces normes varieront certes selon les contextes, mais les éléments listés fourniront une base solide dans tous les contextes :

a) Adresse Web visée : l'adresse Web du contenu collecté, également appelée localisateur ou identificateur uniforme de ressources (URL ou URI), devrait être consignée ;

b) Code source : les enquêteurs doivent saisir le code source HTML de la page Web, le cas échéant. Le code source HTML contient bien plus d'informations que la part visible du site Web. Ce code contribuera à l'authentification des éléments collectés ;

c) Capture pleine page : les enquêteurs devraient d'abord réaliser une capture d'écran de la page Web visée, avec indication de la date et de l'heure, pour disposer de la meilleure représentation possible de ce qui a été vu au moment de la collecte ;

d) Fichiers multimédias intégrés : lorsque la page Web téléchargée contient des vidéos ou des images, par exemple, ces éléments doivent également être extraits et collectés ;

[141] Voir chap. VI.D ci-dessous (Conservation).

e) Métadonnées intégrées : les enquêteurs devraient, le cas échéant, collecter les métadonnées supplémentaires de l'élément numérique. Les métadonnées peuvent varier selon les sources, mais elles comprennent communément les informations suivantes : l'identifiant de l'utilisateur-téléverseur ; l'identifiant de la publication, de l'image ou de la vidéo ; la date et l'heure du téléversement, le géotag, le hashtag, les commentaires et les annotations ;

f) Données contextuelles : le contenu contextuel devrait également être collecté s'il est utile à la bonne compréhension de l'élément numérique. Il pourrait s'agir de commentaires faits concernant une vidéo, une image ou une publication, d'informations sur le téléversement, et d'informations sur le téléchargeur-utilisateur, telles que son nom d'utilisateur, son vrai nom ou sa biographie. L'opportunité de collecter les informations périphériques doit être déterminée sur la base des caractéristiques de l'affaire et de l'élément numérique en question ;

g) Données relatives à la collecte : les enquêteurs en sources ouvertes doivent consigner toutes les données pertinentes relatives à la collecte, telles que le nom de la personne qui collecte, l'adresse IP de la machine utilisée pour ce faire, l'identité virtuelle empruntée, le cas échéant, et l'horodatage. Les enquêteurs devraient s'assurer que l'horloge du système est bien réglée, de préférence en la synchronisant avec un service de protocole de synchronisation réseau, pour que les métadonnées à caractère temporel soient correctement représentées dans les fichiers collectés. S'il est fait usage d'une identité virtuelle pour accéder aux informations collectées, ce fait est à consigner ;

h) Valeur de hachage : les valeurs de hachage sont une forme unique d'identification numérique qui confirme, par voie de cryptographie, que le contenu collecté est unique et n'a pas été modifié depuis le moment de sa collecte. Au point de collecte, les enquêteurs en sources ouvertes devraient ajouter manuellement – ou l'outil de collecte devrait ajouter automatiquement – une valeur de hachage. Il y a de nombreux types de hachages parmi lesquels choisir et les normes en la matière ont évolué au fil du temps. Les enquêteurs devraient faire leur choix en fonction de la norme en vigueur[142].

156. Lorsqu'il y a collecte automatisée, certains des processus décrits peuvent être exécutés par des outils conçus pour recueillir le contenu et les métadonnées voulus. Pour chaque élément collecté, un rapport technique devrait rendre compte des informations ci-dessus afin d'établir l'authenticité de l'élément par la suite. Les informations contextuelles et les métadonnées de tous types devraient toujours être stockés et conservés avec l'élément numérique, comme expliqué dans la section qui suit.

D. Conservation

157. La longévité et la disponibilité des informations en ligne sont souvent précaires. Les plateformes de médias sociaux peuvent retirer des contenus en application de leurs conditions de service, tout comme les utilisateurs peuvent décider de retirer ou de modifier leurs propres mises en ligne. Qui plus est, les informations en ligne peuvent aisément être décontextualisées, perdues, effacées ou altérées[143]. Pour rester accessibles et utilisables aux fins de l'attribution de responsabilités en application de la loi, les éléments numériques doivent être conservés à court terme comme à long terme[144]. Généralement, le but de la conservation numérique est de maintenir l'accessibilité[145]. Lorsqu'il s'agit de préserver des éléments numériques aux fins de l'établissement de responsabilités au regard de la loi, toutefois, le but est de conserver les pièces numériques

[142] Des orientations concernant la norme actuelle sont notamment données par le National Institute of Standards and Technology (États-Unis). Voir www.nist.gov.

[143] Ng, « How to preserve open source information effectively ».

[144] Ibid., p. 143. Voir Organisation des Nations Unies pour l'éducation, la science et la culture, « Concept de préservation numérique ». Disponible à l'adresse https://fr.unesco.org/themes/information-preservation/digital-heritage/concept-digital-preservation.

[145] Ng, « How to preserve open source information effectively ».

d'une manière qui permette d'en assurer l'accessibilité, l'authenticité, l'utilisation éventuelle par des mécanismes d'attribution des responsabilités, et la recevabilité dans le cadre de procédures judiciaires. Aussi la conservation numérique dans le contexte des enquêtes inclut-elle la conservation des informations au fil du temps, de sorte que l'élément collecté reste indépendamment compréhensible pour ses destinataires, qui disposent d'une confirmation suffisante de son authenticité.

158. La conservation à long terme nécessitera peut-être la mise à jour des matériels et formats de stockage pour veiller à ce que les éléments stockés restent accessibles au moyen d'appareils courants.

1. Propriétés de l'élément numérique à protéger et à conserver au fil du temps

159. Selon les archivistes, les propriétés d'un élément numérique qui doivent être protégées et conservées au fil du temps comprennent l'authenticité, la disponibilité, l'identité, la permanence, l'utilisabilité et la compréhensibilité, comme brièvement décrit ci-dessous.

a) Authenticité

160. L'authenticité s'entend de la démonstration du fait qu'un élément numérique est resté inchangé par rapport au moment où il a été collecté. Elle requiert que l'élément numérique ne fasse l'objet d'aucune modification pendant qu'il est archivé, à moins que la modification ne soit dûment consignée[146].

b) Disponibilité

161. La disponibilité s'entend du simple fait qu'un élément numérique continue d'exister et d'être récupérable, et du fait juridique que les conditions sont remplies au regard des droits de propriété intellectuelle pour y accéder et l'utiliser[147].

c) Identité

162. L'identité s'entend du fait que l'élément numérique est référencé. Il doit être identifiable et se distinguer des autres, par exemple en étant associé à un identifiant, tel qu'un numéro d'identification unique[148].

d) Permanence

163. La permanence s'entend de l'intégrité et de la viabilité d'un élément numérique sur le plan technique. Ses séquences de bits doivent être intactes, se prêter au traitement et être récupérables[149].

e) Utilisabilité

164. L'utilisabilité s'entend de la possibilité pour les humains ou les machines d'utiliser un élément numérique ou d'interagir avec lui au moyen de matériels et de logiciels appropriés[150].

f) Compréhensibilité

165. La compréhensibilité s'entend de la possibilité pour les utilisateurs visés d'interpréter et de comprendre un élément numérique[151].

2. Questions propres à l'enquête

166. Les enquêteurs devraient aussi réfléchir et se préparer aux questions propres à l'enquête qui pourraient ou vont se poser pendant le processus de conservation.

a) Chaîne de contrôle

167. La chaîne de contrôle s'entend de la consignation chronologique de la séquence des dépositaires d'un élément d'information ou de preuve, ainsi que la consignation du contrôle, de la date et de l'heure, du transfert, de l'analyse et de la destination d'un tel élément de

146 Id. À noter que l'utilisation du terme « authenticité » dans ce contexte diffère de son utilisation dans un contexte juridique.
147 Id.
148 Id.
149 Id.
150 Id.
151 Id.

preuve. Une fois l'élément numérique collecté, sa chaîne de contrôle doit être maintenue par la mise en place d'un système de conservation numérique en bonne et due forme.

b) Copie admissible en preuve

168. La copie admissible en preuve est l'élément numérique collecté par l'enquêteur ou l'enquêtrice dans sa version originale, dont ni la forme ni le fond ne devraient être modifiés. Les éléments numériques devraient être stockés dans leur version originale. Cela signifie conserver intact un original de l'élément numérique, sous tous les formats rencontrés au moment de la collecte.

c) Copies de travail

169. Une ou plusieurs copies de l'élément numérique devraient être créées à des fins d'analyse, et stockées séparément, de sorte que les enquêteurs puissent s'en servir pour leur travail, sans avoir à utiliser l'original. Cela permet de réduire au minimum les manipulations de l'original et les risques qu'il soit altéré ou modifié. Tout changement touchant l'élément numérique, y compris le fait d'en établir des copies, devrait être consigné. Si possible, des systèmes de stockage séparés devraient être utilisés pour les copies admissibles en preuve et les copies de travail.

d) Stockage

170. Le stockage contribue à la permanence des éléments numériques et à la possibilité de les trouver et de les récupérer. Le stockage ne doit pas se concevoir passivement, mais comme un processus actif comprenant des tâches et des responsabilités continues et dirigées. Il comprend le stockage permanent, dans lequel les supports de stockage jouent un rôle, mais aussi la gestion de la hiérarchie de stockage, le remplacement du support, la vérification des erreurs, le contrôle de la fixité (vérifier que l'élément n'a pas été modifié), la reprise après sinistre, et la localisation et la restitution d'objets stockés[152]. Les informations numériques peuvent être stockées sur place (en ligne ou hors ligne) ou hors site (en ligne ou hors ligne)[153]. Les possibilités de stockage pour les contenus numériques comprennent le disque dur local, le support amovible local, le disque dur en réseau local, le serveur distant ou le système de stockage en nuage (cloud). Les facteurs à considérer pour choisir une solution de stockage sont notamment la capacité de stockage, l'accès et le contrôle, les copies de secours, la législation applicable, ainsi que la sécurité de l'information et la protection des données. Le choix des moyens de stockage doit également prendre en compte la vitesse, la disponibilité, le coût, la viabilité, la gestion du stockage et les systèmes de recherche[154].

i) Copies de secours

171. Lorsque des données sont perdues ou des erreurs se produisent, un archiviste ou un technicien peut tenter de récupérer les données. Idéalement, celles-ci auront fait l'objet d'une copie de secours ou auront été dupliquées en un autre lieu. Les spécialistes en informatique recommandent de disposer d'au moins trois copies des données, sur au moins deux types différents de stockage, dont une copie géographiquement séparée des deux autres.

ii) Dégradation

172. Une des difficultés du stockage réside dans le fait que les supports se dégradent avec le temps. Les archivistes peuvent atténuer le risque d'une perte de stockage en utilisant des types de supports particulièrement durables. Il reste que tout dispositif de stockage finira par présenter un défaut, s'user ou échouer de façon aléatoire. Même sans panne totale, des erreurs de données ou des altérations de fichiers peuvent se produire avec la dégradation des supports. Il est par conséquent important de conserver des copies de secours et de surveiller régulièrement l'infrastructure de stockage et la permanence des fichiers stockés, notamment en vérifiant régulièrement les empreintes

[152] Ibid., p. 154.

[153] Shira Scheindlin et Daniel J. Capra, *Electronic Discovery and Digital Evidence in a Nutshell* (Saint Paul, West Academic Publishing, 2009), p. 21 et 22.

[154] Ng, « How to preserve open source information effectively », p. 156.

numériques d'échantillons pris au hasard, pour vérifier qu'il n'y a pas eu de dégradation.

iii) Obsolescence

173. Les fichiers numériques deviennent obsolètes lorsqu'il devient déraisonnablement difficile d'acquérir ou d'entretenir les matériels nécessaires pour accéder aux données. Quelque durable que puisse être le support de stockage, il risque aussi de devenir obsolète, ce qui rendra difficile, voire impossible, la récupération des données stockées. C'est pourquoi les enquêteurs devraient s'appliquer à entretenir et, quand cela est nécessaire, à remettre à neuf le support de stockage pour maintenir l'utilisabilité et la disponibilité des données collectées.

iv) Restauration

174. Les fichiers numériques peuvent être accidentellement ou intentionnellement supprimés. Lorsqu'un utilisateur « supprime » un fichier sur un ordinateur, le contenu du fichier supprimé restera sur le support de stockage jusqu'à ce qu'un autre fichier vienne l'écraser[155]. Ainsi, plus il y a d'activité sur l'ordinateur ou d'autres supports de stockage, plus vite l'écrasement surviendra et plus vite la restauration deviendra impossible. La plupart des ordinateurs disposent de programmes utilitaires intégrés à leur système d'exploitation qui permettent la restauration de fichiers supprimés. Il existe en outre dans le commerce des logiciels de restauration de données qui peuvent parfois être utilisés pour « restaurer » des fichiers. Les enquêteurs en sources ouvertes devront peut-être s'assurer les services d'informaticiens pour accéder aux données supprimées.

v) Rafraîchissement

175. Le rafraîchissement consiste à copier du contenu d'un support de stockage à un autre. Il ne concerne que l'obsolescence des supports et ne constitue pas une stratégie complète de conservation. Il devrait néanmoins faire partie intégrante de la stratégie globale de conservation[156].

E. Vérification

176. La vérification est le processus par lequel sont établies l'exactitude et la validité des informations collectées en ligne. La vérification des informations de sources ouvertes peut s'effectuer dans le cadre d'une analyse toutes sources – portant également sur les informations de sources fermées et confidentielles – ou d'une analyse portant uniquement sur les sources ouvertes. La vérification s'articule en trois volets, qui sont la source, l'élément ou le fichier numérique, et le contenu, lesquels doivent être considérés collectivement et comparés sous l'angle de la constance.

1. Analyse de la source

177. L'analyse de la source porte sur sa crédibilité et sa fiabilité. L'environnement en ligne est tel qu'il ne facilite pas ce type d'analyse, car nombreuses sont les sources qui sont anonymes ou pseudonymes. Pour bien analyser les sources d'information, les enquêteurs en sources ouvertes doivent d'abord déceler la ou les sources correctes à analyser, c'est-à-dire attribuer les informations à leur source originelle. L'analyse d'attribution consiste à déterminer la source des informations numériques, qui peut être un site Web donné, un abonné ou un utilisateur de tel ou tel compte ou plateforme, ou l'identité des auteurs, créateurs ou téléchargeurs d'un certain contenu. L'analyse d'attribution n'est pas toujours possible et peut nécessiter des investigations supplémentaire en ligne comme dans la réalité, ou encore le recours à des techniques avancées de recherche et d'analyse. Bien qu'il soit utile de savoir qui est l'auteur d'un contenu, le fait de ne pas disposer de ce renseignement n'est généralement pas une lacune critique pour l'établissement de l'authenticité d'un élément en ligne, étant donné qu'il existe d'autres façons d'authentifier des informations de sources ouvertes.

[155] Scheindlin et Capra, *Electronic Discovery and Digital Evidence in a Nutshell*, p. 24.

[156] Cornell University Library, « Digital imaging tutorial ». Disponible à l'adresse http://preservationtutorial.library.cornell.edu/tutorial/preservation/preservation-03.html.

a) Provenance

178. La provenance renvoie à l'origine ou au début connu de l'existence d'une chose. En ce qui concerne les contenus en ligne, la provenance peut désigner soit la première apparition en ligne, soit l'élément original avant qu'il ne soit téléversé sur Internet. En ligne, il vaut mieux parler de « première copie trouvée en ligne » plutôt que de « première copie en ligne », vu que l'original peut avoir été enlevé. Même lorsque les enquêteurs sont convaincus d'avoir trouvé la première version d'une vidéo, par exemple, ou d'autres informations provenant de sources ouvertes en ligne, ils ne peuvent pas avoir la certitude de leur provenance parce qu'il existe par ailleurs des voies fermées, telles que le courriel ou les groupes de messagerie privés, qui pourraient avoir été utilisés pour partager l'élément avant qu'il n'apparaisse en ligne, aux yeux du public[157].

b) Crédibilité

179. L'historique de publication en ligne, l'activité en ligne et la présence sur Internet d'une source peuvent contenir des informations utiles qui pourraient jouer en faveur de sa crédibilité ou contre celle-ci. Les enquêteurs devraient examiner la présence en ligne et l'historique d'affichage d'une source, ces précautions pouvant même contribuer à déjouer une éventuelle tentative de supercherie. À supposer, par exemple, que la source publie un contenu sur des faits survenus dans un pays donné, est-ce que ses autres publications du moment donnent à penser qu'elle est effectivement dans ce pays ?

c) Indépendance et impartialité

180. Les enquêteurs devraient se pencher sur la question de l'impartialité de la source. Ils peuvent le faire en regardant de quels groupes et organisations les personnes concernées sont proches, en relevant les autres affiliations qu'elles pourraient avoir, en s'intéressant à leurs sources de revenus et de financement, et en posant la question de savoir si elles ont des connexions ou des relations avec une quelconque partie à l'affaire ou aux faits concernés. Pour se prononcer sur l'indépendance des sources, il convient donc de déterminer si elles pourraient être associées à des entités concernées (par exemple, une partie au conflit). L'idéologie d'une source et son appartenance à tout groupe pourraient également être d'importance. Pour toutes les sources, les enquêteurs devraient rechercher et établir leurs mobiles, intérêts ou programmes sous-jacents, ainsi que la mesure dans laquelle ceux-ci pourraient influencer la véracité de ce qu'elles publient.

d) Spécificité

181. Plus les informations et les prétentions seront précises, plus il sera aisé de les confirmer ou de les infirmer. Les assertions générales et vagues tendent à être plus difficiles à apprécier de façon critique.

e) Atténuation

182. Les textes rédigés au moment des faits auxquels ils se rapportent auront tendance à être pris pour plus fiables que ceux qui ont été produits longtemps après[158]. Ce facteur peut s'avérer problématique pour les enquêteurs en sources ouvertes lorsque la date de création d'un texte numérique n'est pas claire.

2. Analyse technique

183. L'analyse est dite technique lorsqu'elle porte sur l'élément numérique lui-même, qu'il s'agisse d'un document, d'une image ou d'une vidéo. Afin de mettre à l'épreuve l'intégrité d'un fichier, c'est-à-dire de déterminer s'il peut avoir été numériquement altéré, manipulé ou modifié, les enquêteurs en sources ouvertes auront peut-être intérêt à le soumettre à un examen de criminalistique numérique, parfois appelé « digital investigative analysis » (analyse numérique d'enquête). Les composantes d'un tel examen sont présentées ci-dessous.

[157] Par exemple, un utilisateur envoie une photographie par courriel à un autre utilisateur, qui la téléverse ensuite sur un média social. C'est l'expéditeur du message électronique qui est à l'origine de la photographie et non la personne qui l'a publiée.

[158] Institute for International Criminal Investigations, *Investigators Manual*, 5e éd. (La Haye, 2012), p. 88.

a) Métadonnées

184. Les métadonnées sont des données qui décrivent d'autres données et fournissent des informations à leur sujet. Elles peuvent être créées par l'utilisateur qui a produit un élément, par d'autres utilisateurs, par un prestataire de services de communication ou par tout appareil sur lequel des données sont générées, transférées, reçues ou affichées. Elles sont utiles pour la description d'un élément et les circonstances de sa création, de sa diffusion et de sa modification. Elles peuvent inclure le créateur et la date de création du fichier, des données relatives à son téléversement, ses modifications et sa taille, et des géodonnées. Les métadonnées peuvent être intégrées dans un fichier, visibles sur une page Web ou présentes dans un code source. Certaines métadonnées peuvent être ôtées avant ou pendant le téléversement, ou par suite de l'utilisation d'applications de médias sociaux. Si elles sont disponibles, toutefois, elles devraient être examinées afin de déterminer si elles pourraient contribuer à établir l'authenticité de l'élément. Les métadonnées d'origine peuvent être perdues parce que les plateformes transcodent souvent les médias téléversés pour en optimiser la visualisation, le partage ou la lecture en ligne. Dans ces cas, les métadonnées correspondront au nouveau fichier, et non à l'original. Lorsque les métadonnées ont été ôtées, les enquêteurs en sources ouvertes devraient rechercher d'autres moyens de vérifier un élément.

b) Format de fichier d'image échangeable

185. Les données du format de fichier d'image échangeable (exchangeable image file format) sont un type de métadonnées qui précisent les formats des images, des sons et des balises utilisés par les caméras, les scanneurs et les autres systèmes numériques qui traitent des fichiers image et son enregistrés par appareils numériques.

c) Code source

186. Le code source constitue la programmation de toute page Web ou de tout logiciel. Dans le cas des sites Web, ce code peut être visualisé par tout un chacun muni de certains outils ou même de leur simple navigateur. Le code source d'un site Web est aisé à visualiser au moyen de plusieurs outils librement disponibles. Il peut comporter du métacontenu ou du contenu caché ou manipulé, et montrera la structure des liens ainsi que les liens rompus.

3. Analyse de contenu

187. L'analyse de contenu est le processus par lequel les informations contenues dans une vidéo, une image, un document ou une déclaration sont appréciées en matière d'authenticité et de véracité. Il s'agit d'un processus à multiples facettes qui consiste notamment à analyser des indices visuels ou à corroborer l'image avec les métadonnées. Sur de nombreux points, les caractéristiques de l'environnement en ligne peuvent affecter la validité et la véracité réelles ou perçues des informations de sources ouvertes qui s'y trouvent. Parmi ces points figurent le phénomène des références circulaires ou citogenèse, la décontextualisation des informations et la mésinterprétation. Les données de contenu sont des données qui se trouvent dans l'élément numérique, qui peut être une vidéo, une image, un enregistrement audio, un document ou un texte non structuré.

a) Identifiants uniques

188. Lorsqu'ils sont appelés à vérifier un contenu visuel, les enquêteurs devraient commencer par rechercher des traits uniques ou identifiants. Il peut s'agir de constructions, de plantes et d'animaux, de personnes, de symboles et d'insignes. Il doivent faire particulièrement attention lorsqu'ils analysent des physionomies humaines dans

le but d'identifier une personne précise[159]. Les pratiques d'identification nécessitent habituellement des compétences particulières, telles que celles acquises au fil du temps et moyennant une formation perfectionnée par les spécialistes en criminalistique. Les analyses non professionnelles peuvent s'avérer inexactes, préjudiciables ou autrement problématiques si elles sont effectuées par des professionnels non formés en la matière.

b) Informations objectivement vérifiables

189. Il peut souvent être utile de commencer par cerner ce qui pourrait constituer des « informations objectivement vérifiables ». Par exemple, le temps qu'il faisait un jour donné, le nom et le grade d'un commandant, ou l'emplacement d'un immeuble, sont des informations qui pourraient toutes être objectivement vérifiables. L'appréciation des éléments de sources ouvertes devrait comprendre un examen de leurs contenus au regard de telles informations objectivement vérifiables.

c) Géolocalisation

190. La géolocalisation est la détermination ou l'estimation de l'emplacement d'un objet, d'une activité ou de l'origine d'un élément. Il pourrait être possible, par exemple, d'utiliser des techniques de géolocalisation pour déterminer le lieu qui figure dans une vidéo ou sur une photographie téléchargée d'Internet. Les techniques en question peuvent consister, par exemple, à mettre en corrélation les caractéristiques géographiques uniques qui apparaissent sur une photo avec leur emplacement effectif sur une carte.

d) Chronolocalisation

191. La chronolocalisation est la corroboration des dates et des heures associées aux faits représentés dans des informations qui sont habituellement de nature visuelle. Il pourrait être possible, par exemple, de déterminer le moment de la journée où une photographie a été prise en examinant la longueur des ombres produites par la lumière du soleil, en conjonction avec d'autres indicateurs.

e) Complétude

192. Un document incomplet ou une séquence vidéo tronquée peuvent conserver une certaine valeur probante, mais les lacunes que l'élément présente peuvent avoir une incidence sur le poids qui pourra lui être accordé. C'est pourquoi il est important, lorsque sont collectées des informations en sources ouvertes, de saisir le fichier visé dans sa totalité et, le cas échéant, de saisir le contexte environnant.

f) Cohérence interne

193. L'appréciation de la cohérence interne peut se faire sur la base d'un seul élément d'information provenant d'une source ouverte en ligne ou d'un ensemble d'éléments provenant d'une source donnée (ou de sources ayant la même provenance ou les mêmes auteurs). L'appréciation de la cohérence interne d'un seul élément d'information en ligne sert à établir si l'information est cohérente en soi. Il y a cohérence interne, lorsque l'élément d'information ou l'ensemble d'éléments d'information ne se contredisent pas eux-mêmes.

g) Corroboration externe

194. La corroboration externe est le fait d'informations qui existent à l'extérieur d'un élément numérique mais qui correspondent à son contenu et tendent donc à en confirmer la véracité.

[159] L'analyse criminalistique et l'identification des physionomies humaines, avec ou sans outils (par exemple, reconnaissance faciale, analyse de la démarche, etc.), nécessitent l'intervention de spécialistes en criminalistique. Voir Nina M. van Mastrigt et al., « Critical review of the use and scientific basis of forensic gait analysis », *Forensic Sciences Research*, vol. 3, n° 3 (2018), p. 183 à 193 (disponible à l'adresse www.tandfonline.com/doi/full/10.1080/20961790.2018.1 503579) ; Royal Society and Royal Society of Edinburgh, « Forensic gait analysis: a primer for courts » (Londres, 2017) (disponible à l'adresse https://royalsociety.org/-/media/about-us/programmes/science-and-law/royal-society-forensic-gait-analysis-primer-for-courts.pdf). Voir aussi European Network of Forensic Science, *Best Practice Manual for Facial Image Comparison* (2018) (disponible à l'adresse http://enfsi.eu/ wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf) ; National Center for Audio and Video Forensics, « Height analysis of surveillance video » (disponible à l'adresse https://ncavf.com/what-we-do/forensic-height-analysis).

F. Analyse d'enquête

195. L'analyse d'enquête est la pratique qui consiste à examiner et à interpréter les informations portant sur les faits pour en dégager des constatations et des conclusions de fond dans le cadre d'un processus décisionnel ou de la constitution d'un dossier. Le volume et la qualité des informations de sources ouvertes étant variables, l'analyse doit être bien structurée.

196. Avant d'être soumises à certains types d'analyse, les informations de sources ouvertes devront peut-être être traitées. Ce traitement peut consister à traduire celles qui sont dans d'autres langues que les langues de travail, ou à regrouper différents ensembles de données pour contribuer à l'analyse de comportements, de lieux, d'objets, de relations ou de réseaux, de mouvements, d'activités ou de transactions. Il peut également consister à modifier la nature ou le format d'un élément numérique pour le rendre compatible avec tel ou tel logiciel. Les opérations suivantes comptent parmi les types communs de traitements de données :

a) Traduction : lorsque des données sont dans une langue qui n'est pas parlée par les enquêteurs ou qui n'est pas traitée par le logiciel nécessaire pour examiner les informations, les données peuvent avoir à être traduites avant de passer aux étapes suivantes ;

b) Regroupement : les enquêteurs devront peut-être regrouper différents ensembles de données en un ensemble plus grand afin de l'analyser ;

c) Reformatage : pour faciliter les recherches dans les données ou la récupération de données, les enquêteurs auront peut-être à changer le format d'un élément numérique.

197. Il est conseillé de ne traiter que les copies de travail d'un élément numérique, et non son original ou sa copie admissible en preuve. Tout traitement d'un élément numérique devrait être consigné. Si les enquêteurs ont recours à des technologies numériques pour traiter les données, comme l'analyse au moyen d'algorithmes, notamment le traitement du langage naturel et l'apprentissage profond, ils doivent être conscients des biais qui peuvent se manifester dans le traitement de ce type de données.

198. Une fois traitées, les informations peuvent être analysées. Les produits de l'analyse des informations de sources ouvertes varieront selon l'objet du travail, la nature et la portée des informations collectées, le calendrier de production et le public visé. Les produits seront mis au point pour répondre aux besoins de l'enquête et pourraient inclure des diagrammes, résumés, glossaires, dictionnaires et des aides visuelles telles que des cartes et des exercices de cartographie[160].

199. Les enquêteurs devraient appliquer des normes rigoureuses pour assurer l'objectivité, la présentation en temps voulu, la pertinence et l'exactitude des données, constatations et conclusions contenues dans les produits analytiques, ainsi que pour protéger le droit à la vie privée et prendre en compte d'autres considérations relatives aux droits, surtout lorsque des informations peuvent conduire à l'identification de personnes. De telles informations ne devraient figurer que dans des produits pour lesquels les enquêteurs ont obtenu le consentement des personnes concernées et seulement si elles sont directement utiles à l'enquête. Elles devraient également être considérées au regard des restrictions de nature déontologique et juridique qui affectent l'utilisation[161].

200. Les sections suivantes présentent des types courants d'analyses qui pourraient servir les objectifs d'une enquête en sources ouvertes.

1. Analyse de comparaison d'images et de vidéos

201. L'analyse de comparaison est le processus par lequel les caractéristiques d'objets, de personnes ou de lieux sont comparées à d'autres éléments inconnus ou connus, alors qu'au moins un des éléments en question est une image. Il s'agit d'analyser le contenu des images et des

[160] Voir chap. VII ci-dessous (Rapport d'enquête).

[161] Voir chap. III ci-dessus (Cadre juridique).

vidéos, notamment les points de comparaison entre différents éléments et caractéristiques, ainsi que leur qualité et leurs réglages visuels (luminosité, perspective, etc.). Bien que de nombreux non professionnels connaissent les bases de l'analyse de comparaison d'images, l'assistance spécialisée d'une personne qualifiée et certifiée en analyse vidéo criminalistique ou en criminalistique numérique pourrait s'avérer utile pour effectuer une analyse scientifique assortie d'un avis d'expert. D'autres enquêtes, dont celles relatives aux droits de l'homme, pourraient également bénéficier d'une telle expertise qui donnerait un poids supplémentaire à leurs constatations et conclusions.

2. Analyse d'interprétation d'images et de vidéos

202. L'analyse d'interprétation d'images et de vidéos, apparentée à l'analyse de comparaison d'images et de vidéos, consiste à analyser un élément numérique pour en comprendre le contenu visuel. Il s'agit d'analyser, pour ne citer que quelques exemples, les coups de feu, les blessures, le sang, les véhicules, les armes et les moyens militaires qui pourraient apparaître dans un tel document, ou encore de calculer la vitesse d'un véhicule ou l'âge d'un individu qui y figurent. Ce travail peut être effectué par des analystes à des fins d'enquête ou par des spécialistes de la criminalistique ou des matières concernées s'agissant d'établir des faits en justice ou de dégager des conclusions en matière de droits de l'homme.

3. Analyse spatiale

203. L'analyse spatiale ou géospatiale peut notamment consister à analyser le contenu visuel et les métadonnées d'éléments auxquels sont associés des coordonnées géographiques ou des noms de lieux. Il s'agit d'examiner différents objets et différentes caractéristiques du paysage, à la résolution voulue, en se servant d'images satellites ou autres, de géodonnées, de cartes, d'une bonne connaissance de l'affaire et de son contexte, et d'outils relatifs aux systèmes d'information géographique[162].

4. Cartographie des acteurs

204. La cartographie des acteurs est une technique qui sert à se faire une idée des principaux acteurs en présence et des relations de pouvoir et voies d'influence en jeu[163]. Il s'agit donc d'abord de repérer les principaux acteurs, puis de cartographier les relations qui existent entre eux.

5. Analyse des réseaux sociaux

205. Dans le même ordre d'idées que la cartographie des principaux acteurs, l'analyse des réseaux sociaux consiste à dresser la carte et à prendre la mesure des relations qui existent entre les personnes, les groupes, les organisations, les ordinateurs, les URL et d'autres entités connectées dans les domaines de l'information ou des connaissances[164]. Les personnes et les groupes sont souvent considérés comme étant les nœuds de ces configurations, les liens représentant les relations qui existent entre ces nœuds. L'analyse des réseaux sociaux utilise les connexions établies sur les médias sociaux et d'autres plateformes mobiles du Web pour déterminer et comprendre les relations qui existent entre les individus. Cette analyse des connexions et des liens peut être effectuée manuellement par l'enquêteur ou l'enquêtrice, ou confiée à des logiciels d'analyse.

6. Cartographie des faits

206. La cartographie des faits est une technique d'analyse qui sert à établir les rapports temporels et géographiques qui existent entre différents faits. Dans le contexte des violations du droit pénal international et du droit international des droits humains, il peut s'agir du lieu de ces infractions ainsi que de faits antérieurs et postérieurs. Il peut également être question de cartographier d'autres faits connexes, notamment de situer dans l'espace et dans le temps des déclarations faites par les auteurs présumés.

[162] Le système d'information géographique est une base de données informatisée pour la gestion et l'analyse des données spatiales.

[163] OHCHR, *Manual on Human Rights Monitoring*, chap. 8 (Analysis), p. 24.

[164] Orgnet, « Social network analysis: an introduction ». Disponible à l'adresse www.orgnet.com/sna.html.

7. Analyse des formes de criminalité et de violations

207. Dans le contexte de l'application des lois au niveau national, une forme de criminalité est un groupe de deux infractions pénales ou plus qui ont été signalées aux forces de l'ordre ou qui ont été découvertes par celles-ci et qui sont uniques en ce qu'elles ont en commun au moins un des aspects suivants : le type d'infraction, le comportement des auteurs ou des victimes, certaines caractéristiques des auteurs, des victimes ou des cibles, les biens substitués, et le lieu des faits[165]. De même, des formes de criminalité ou de violations peuvent être établies dans des affaires relevant du droit pénal international et du droit international des droits humains sur la base d'informations de sources ouvertes.

[165] International Association of Crime Analysts, « Crime pattern definitions for tactical analysis », *Standards, Methods and Technology Committee White Paper 2011-01*, p. 1.

VII

RAPPORT D'ENQUÊTE

SOMMAIRE DU CHAPITRE

- Les constatations et les conclusions de l'enquête en sources ouvertes, qu'il s'agisse des données collectées ou des conclusions dégagées de ces données, peuvent être communiquées oralement, visuellement ou par écrit.
- Les enquêteurs devraient se demander quel format est le plus adapté à leur mandat et au public visé – compte tenu de facteurs comme les connaissances technologiques du public, l'accessibilité, l'objectivité, la transparence et la sécurité – lorsqu'ils choisissent : a) le ou les formats à utiliser ; et b) les données à inclure.

208. Le présent chapitre examine les façons dont il peut être rendu compte des enquêtes en sources ouvertes, avec leurs méthodes, leurs données brutes et leurs conclusions analytiques. Dans de nombreux cas, les informations de sources ouvertes seront présentées en tandem avec d'autres informations recueillies par d'autres méthodes d'enquête. La présentation peut prendre diverses formes : rapport écrit, rapport oral, rapport visuel ou toute combinaison de ces trois formes. Les rapports peuvent être à usage interne ou pour publication externe, et peuvent être considérés comme des rapports d'experts ou non selon un certain nombre de facteurs. Les rapports devraient présenter les garanties suivantes :

a) Exactitude : les rapports devraient rendre compte avec exactitude des données collectées[166]. Les informations à décharge devraient être incluses, ainsi qu'une explication de tout caviardage ou toute lacune ;

b) Attribution : les rapports devraient établir une distinction claire entre la matière qui relève du domaine public ou les informations générales non classifiées, les informations qui sont classifiées ou dont la diffusion est restreinte, et la matière qui reflète le jugement ou l'avis des enquêteurs ou d'autres professionnels. Les enquêteurs ou les autres parties qui rapportent des informations de sources ouvertes devraient également prendre les précautions voulues et obtenir les permissions nécessaires pour utiliser des contenus qui pourraient appartenir à d'autres, notamment en obtenant les droits de propriété intellectuelle requis ;

c) Complétude : les constatations et les conclusions devraient indiquer dans quelle mesure les données rapportées sont complètes, surtout si certaines ont été délibérément exclues ;

d) Confidentialité : bien que les rapports relèvent de la sphère des sources ouvertes, leurs auteurs devraient se poser la question de savoir quelles informations devraient être exclues ou caviardées pour protéger la confidentialité ou réduire au minimum d'autres risques, notamment ceux que pourraient courir les sources, les témoins, les victimes et les membres des communautés qui ont un lien avec les informations de sources ouvertes ;

e) Langue : les auteurs des rapports devraient utiliser une langue neutre et éviter toute formulation émotionnelle ou affective. Ils devraient énoncer les faits clairement sans abuser de l'adjectif et sans emphase. Les rapports doivent être écrits dans le souci de l'égalité des genres. Idéalement, s'ils sont publics, ils devraient être disponibles dans les langues des communautés affectées, outre les langues officielles utilisées par les enquêteurs ou les entités d'enquête ;

f) Transparence : les auteurs des rapports devraient indiquer clairement comment les enquêteurs ont travaillé, selon quels objectifs, processus et méthodes. Normalement, ces informations devraient figurer dans la partie du rapport consacrée à la méthodologie, mais elles devraient aussi guider les descriptions d'un bout à l'autre du texte. Les descriptions devraient être aussi transparentes que possible sans créer de vulnérabilités de sécurité, par la révélation d'informations confidentielles, par exemple.

A. Rapport écrit

209. L'enquête en sources ouvertes peut être présentée par écrit, dans le cadre de rapports internes, de rapports destinés à des clients et de rapports publics. Les conclusions analytiques peuvent ainsi être communiquées au moyen d'un rapport écrit. On peut notamment trouver dans cette catégorie des rapports d'ONG, de commissions d'enquête, de missions d'établissement des faits et des Nations Unies, ainsi que des rapports d'experts destinés aux tribunaux[167]. Les informations de sources

[166] Voir chap. II.B ci-dessus (Principes méthodologiques).

[167] Pour un exemple de rapport écrit sur une enquête en sources ouvertes numériques, voir, par exemple, Human Rights Investigations Lab, « Chemical strikes on Al-Lataminah: March 25 & 30, 2017 – a student-led open source investigation » (Berkeley, Human Rights Center, Faculté de droit de l'Université de Californie à Berkeley, 2018).

ouvertes numériques seront souvent intégrées à d'autres formes de données et d'analyses de sources ouvertes et fermées. Les rapports écrits devraient analyser les informations collectées de sorte à en dégager des conclusions, des estimations et des prédictions logiques. Les rapports devraient dénoter d'une solide méthodologie qui doit pouvoir être expliquée au public visé. La véracité et l'intégrité des informations sous-jacentes sont cruciales pour un rapport. De mauvaises données donnent de mauvaises constatations et conclusions[168].

210. Les rapports écrits doivent comporter les sections suivantes, à moins qu'un motif justifié et énoncé ne s'y oppose, pour éviter de divulguer certaines techniques, méthodes et sources d'enquête qui doivent rester confidentielles, par exemple :

a) Objectifs : le rapport devrait fournir les objectifs de l'enquête ainsi que les mandats ou les instructions des clients qui les sous-tendent, y compris les questions de recherche bien définies et clairement énonçables ;

b) Méthodologie : le rapport devrait fournir les méthodes de recherche de l'enquête pour qu'elles puissent être reproduites et pour permettre au public de comprendre et apprécier la crédibilité des informations, constatations et conclusions de l'enquête, y compris ce qui est couvert ;

c) Activités : le rapport devrait comporter un résumé des activités qui ont été menées et qui sont importantes pour les constatations et les conclusions dégagées ou pour apprécier la qualité de l'analyse, y compris les activités menées pour relever les données sous-jacentes, ce qui a été collecté et ce qui a été analysé ;

d) Données et sources : le rapport devrait comporter une description des données sous-jacentes, y compris de leurs sources et de leur qualité ;

e) Lacunes et incertitudes : le rapport devrait relever toute lacune ou incertitude relative aux données sous-jacentes ou à l'analyse qui pourrait avoir une importance pour les constatations et les conclusions ;

f) Résultats et recommandations : le rapport devrait rendre compte de la façon dont les enquêteurs ont interprété les données ou les constatations et conclusions dégagées de l'analyse des données, en indiquant les réserves et les nouvelles pistes.

B. Rapport oral

211. Lorsque les constatations et les conclusions d'une enquête en sources ouvertes atteignent le prétoire, les enquêteurs peuvent être amenés à déposer en tant que témoins et, partant, à rendre compte de leurs travaux d'enquête à la barre. Ils peuvent avoir à faire de même dans des exposés devant des commissions de vérité, des forums d'ONG, des tribunaux populaires ou des manifestations médiatiques.

212. Tout enquêteur qui doit présenter oralement les constatations et les conclusions de son enquête en sources ouvertes doit être en mesure d'expliquer avec clarté et sans erreur en quoi a consisté le travail d'enquête, notamment les méthodes et les outils qui ont été utilisés. Ainsi, la déposition orale et les constatations et conclusions décrites se verront accorder le poids qu'elles méritent.

213. Dans les procédures judiciaires, ce sont souvent les chefs des enquêtes qui seront entendus. Ils devront donc être en mesure de parler du travail de leurs équipes. Pour cela, il faut bien entendu qu'ils sachent ce que leurs équipes ont fait et qu'ils puissent répondre aux questions sur les rôles joués et les raisonnements suivis pour prendre des décisions concernant la portée de l'enquête, ses méthodes, les outils utilisés, etc. Les enquêteurs peuvent comparaître en tant que témoins experts ou simples témoins. Les témoins experts – c'est-à-dire les témoins

[168] Selon les circonstances et les exigences de confidentialité, l'examen par les pairs est recommandé pour veiller à l'exactitude et à la qualité des données et des constatations, de l'analyse et des conclusions fondées sur ces données.

qui ont cette qualité du fait de leur expérience professionnelle, de leurs connaissances, de leurs compétences, de leur formation ou de leurs qualifications connexes – sont habilités à parler des conclusions qu'ils ont dégagées et d'autres résultats analytiques du travail d'enquête, tandis que les témoins ordinaires doivent généralement s'en tenir aux faits, et plus précisément à ceux qu'ils ont personnellement observés.

C. Rapport visuel

214. La visualisation des données est la représentation graphique d'informations sous la forme, notamment, de diagrammes, de graphiques, de tableaux, de cartes et d'infographies. C'est une façon accessible de voir et comprendre les tendances, les valeurs aberrantes et les constantes dans les données[169]. Elle peut notamment comporter des diagrammes et d'autres représentations graphiques des données dans l'espace et le temps, des diagrammes (dont ceux qui illustrent les connexions, tendances et relations mathématiques), des graphes de réseaux qui représentent les relations parmi diverses personnes, et des diagrammes statistiques. Les cartes bi- et tridimensionnelles représentant les objets dans l'espace et le temps, et les reconstructions en trois dimensions de divers sites, dont des lieux de crimes, font également partie du répertoire des moyens de visualisation[170]. Ces outils peuvent s'avérer utiles pour comprendre de grandes quantités de données, une situation courante dans le cas des enquêtes en sources ouvertes, ou pour mieux saisir les faits constitutifs de situations complexes.

215. Il existe d'autres types de visualisation des données :

a) Cartes mentales : une carte mentale est un moyen graphique de représenter des idées et des concepts et les relations qui existent entre eux. Les cartes mentales structurent les informations d'une manière qui en facilite l'analyse, la synthèse et la compréhension. Les cartes mentales comprendront souvent une explication de la découverte des données sous-jacentes ;

b) Diagrammes de décision : un diagramme de décision est la représentation graphique d'une séquence de faits, tels que les étapes d'un algorithme, l'organisation des tâches ou des processus similaires ;

c) Infographies : une infographie est une représentation illustrée d'une idée ou d'un concept ; elle peut servir à représenter des informations statistiques.

216. Les informations de sources ouvertes peuvent être représentées de multiples façons allant de la simple présentation audiovisuelle d'une vidéo ou d'un site Web à des présentations multimédia interactives, numériques et composites[171]. Les démonstrations et les illustrations visuelles, ou les plateformes numériques, peuvent être utilisées pour présenter les informations d'une façon qui permette aux publics visés

[169] Exemples de rapports visuels utilisés dans divers contextes : plateformes numériques présentées à titre de preuve démonstrative dans *Le Procureur c. Ahmad Al Faqi Al Mahdi* à la Cour pénale internationale et dans *Le Procureur c. Salim Jamil Ayyash et consorts* au Tribunal spécial pour le Liban ; *Report of the detailed findings of the independent international commission of inquiry on the protests in the Occupied Palestinian Territory* (disponible à l'adresse www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session40/Documents/A_HRC_40_74_CRP2.pdf) ; BBC Africa Eye, « Cameroon atrocity: what happened after Africa Eye found who killed this woman », BBC News, 30 mai 2019 (disponible à l'adresse www.bbc.com/news/av/world-africa-48432122/cameroon-atrocity-what-happened-after-africa-eye-found-who-killed-this-woman). Voir aussi, de façon générale, les travaux de Forensic Architecture et SITU Research.

[170] Voir, par exemple, International Criminal Court Digital Platform: Timbuktu, Mali (plateforme conçue par SITU Research pour l'affaire *Al Mahdi* de la Cour pénale internationale). Disponible en ligne à l'adresse http://icc-mali.situplatform.com. Voir aussi la variété d'enquêtes en sources ouvertes en ligne et leurs rapports visuels réalisés par Forensic Architecture (disponible à l'adresse https://forensic-architecture.org/methodology/osint).

[171] Quoique dans un contexte non judiciaire, la Visual Investigations Team du *New York Times* a produit un certain nombre d'explicatifs visuels conçus pour rassembler des informations de sources ouvertes en ligne sur des faits complexes, faciliter l'analyse de ces faits et présenter des conclusions à leur sujet. Voir, par exemple, Nicholas Casey, Christoph Koettl et Deborah Acosta, « Footage contradicts U.S. claim that Nicolás Maduro burned aid convoy », New York Times, 10 mars 2019 (disponible à l'adresse www.nytimes.com/2019/03/10/world/americas/venezuela-aid-fire-video.html) ; Malachy Browne et al., « 10 minutes. 12 gunfire bursts. 30 videos. Mapping the Las Vegas massacre », *New York Times*, 21 octobre 2017 (disponible à l'adresse www.nytimes.com/video/us/100000005473328/las-vegas-shooting-timeline-12-bursts.html).

de comprendre plus facilement les faits sous-jacents. Les lignes de temps, les photographies composites (comme la vue à 360 degrés d'un lieu de crime) et les vidéos montées sont des exemples.

217. Lorsqu'il s'agit de présenter des visualisations de données et des éléments de preuve en multimédia devant un tribunal ou devant d'autres assemblées publiques, les enquêteurs devraient comprendre quelles questions techniques pourraient se poser, notamment celle de savoir de quelles plateformes les avocats pourraient avoir besoin pour rendre leurs exposés aussi utiles que possibles pour les juges des faits. Une série de facteurs doivent être pris en compte pour décider de la meilleure façon de présenter les données sous-jacentes. Parmi ces facteurs figurent les publics visés et la mesure dans laquelle ils sont à l'aise avec les formats possibles, leur capacité de comprendre les informations communiquées[172]. En définitive, toutes les présentations devraient servir à éclairer les faits d'une affaire de façon probante et non préjudiciable, dans le respect des exigences déontologiques et juridiques de la juridiction saisie.

[172] Voir Alexa Koenig, « Open source evidence and human rights cases: a modern social history », dans *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation and Accountability*, Sam Dubberley, Alexa Koenig et Daragh Murray, dir. (Oxford, Oxford University Press, 2020), p. 38 à 40.

VIII

GLOSSAIRE

SOMMAIRE

- Termes et définitions utilisés dans les enquêtes en sources ouvertes ou dans les ressources concernées.

218. Le présent chapitre contient des termes et des définitions qui peuvent être utiles aux enquêteurs en sources ouvertes. Certains de ces termes ne sont pas utilisés dans le présent Protocole, mais sont inclus parce qu'ils peuvent se rencontrer dans les ressources se rapportant aux enquêtes.

Adresse de protocole Internet (IP) : tout appareil numérique qui se connecte à Internet dispose d'une adresse IP. Il y a deux types d'adresses IP : IPv4 (nombre de 32 bits) et IPv6 (nombre de 128 bits). L'adresse IP peut servir à identifier les ordinateurs et les autres appareils sur Internet.

Adresse URL : l'endroit où se trouve une page Web sur Internet. C'est l'équivalent d'une adresse Web.

Algorithme (algorithm) : une procédure ou une série d'instructions bien définies qui permettent à un ordinateur de résoudre un problème ou de réagir à un scénario prédéterminé.

Anonymisation (anonymization) : le processus qui consiste à rendre impossible l'identification d'un individu donné.

Apprentissage automatique (machine learning) : un type d'intelligence artificielle qui utilise des techniques statistiques pour doter les ordinateurs de la faculté d'« apprendre » à partir de données, sans être spécialement programmés.

Archive numérique (digital archive) : une collection de documents, de pages Web ou de registres électroniques. L'expression peut aussi désigner une structure formelle ou informelle qui accepte la responsabilité de conserver des informations et de les mettre à la disposition des utilisateurs autorisés.

Captcha : acronyme de l'anglais « completely automated public Turing test to tell computers and humans apart » qui désigne un type de test utilisé en informatique pour déterminer si un utilisateur est humain.

Chaîne de blocs (blockchain) : une technologie fondée sur la cryptographie selon laquelle un registre distribué et ouvert, constitué de « blocs », peut être utilisé pour enregistrer des transactions entre deux parties ou entités de façon efficace, vérifiable et permanente.

Collecteur (ou robot d'indexation (Web crawler) : programme qui parcourt systématiquement Internet selon un script automatisé pour télécharger et indexer les sites Web visités.

Conservation numérique (digital preservation) : les politiques et les stratégies requises pour gérer et préserver au fil du temps des informations numériques dont la valeur est durable, de sorte que leurs utilisateurs puissent les récupérer et les utiliser à l'avenir.

Cookie (ou témoin de connexion) : un petit fichier de données qui, envoyé par un site Web, s'installe dans la mémoire de l'ordinateur de l'utilisateur ou s'écrit sur le disque d'un ordinateur pour être utilisé par un navigateur. Les cookies sont souvent nécessaires au fonctionnement correct d'un site Web. Ils permettent, par exemple, l'enregistrement des préférences et des identifiants des utilisateurs du site pour leur éviter d'avoir à saisir ces données à chaque visite subséquente.

Cryptage (encryption) : le processus qui consiste à rendre les données inaccessibles sans une clef de déchiffrement.

Cryptographie (cryptography) : la pratique consistant à encoder ou décoder numériquement des informations.

Dark Web : cette partie d'Internet qui n'est accessible qu'au moyen de logiciels spéciaux, permettant aux utilisateurs et aux opérateurs de sites Web de rester anonymes et indétectables.

Données intégrées (embedded data) : données contenues dans un fichier source ou une page Web.

Données non structurées (unstructured data) : données ou informations qui se présentent sous de nombreuses formes, qui ne sont pas organisées selon un format strict, et qui ne sont donc pas facilement traitées et analysées. Elles se présentent habituellement sous la forme de texte, mais il peut aussi s'agir de fichiers image, audio et vidéo.

Données relatives au trafic (traffic data) : toutes données traitées dans le but d'obtenir des informations sur un réseau de communication électronique ou d'établir la facturation d'une telle communication. Ces données portent également sur le routage, l'heure ou la durée de la communication.

Données structurées (structured data) : données ou informations incluses dans un répertoire selon un format strict (il s'agit habituellement d'une base de données, mais il pourrait aussi s'agir d'un ensemble de formulaires complétés), de sorte que leurs éléments puissent être directement traités et analysés.

Dragnet : en ligne, une vaste collection automatisée ou un système de surveillance.

Espace d'air virtuel (air gap) : s'emploie lorsqu'un appareil numérique n'est pas directement connecté à Internet ni à un réseau, pour sécuriser les informations qu'il contient.

Fichier natif (native file) : un fichier sous son format originel.

Format PDF : un format de fichier dont la mise en page fixe préserve le format des documents (y compris les polices, les espacements et les images), quels que soient le logiciel, le matériel et le système d'exploitation utilisés pour les ouvrir et les voir. Le fait de conversion un fichier de son format originel au format PDF lui ôte ses métadonnées et créé une image statique du document.

Forum de discussion (Internet forum) : un site Web par l'intermédiaire duquel les utilisateurs peuvent afficher des messages et avoir des conversations. Les forums contiennent habituellement des messages plus longs que ceux des salons de discussion et sont plus susceptibles d'archiver le contenu du site.

Fournisseur d'accès à Internet (Internet service provider (ISP)) : une entité qui fournit aux utilisateurs d'Internet les services leur permettant d'accéder à Internet et de l'utiliser.

Fournisseur de services sur le Web (Web-based service provider) : une entité qui fournit des services et des produits sur Internet, par exemple les prestataires de médias sociaux.

Hachage ou valeur de hachage (hash ou hash value) : calculs qui peuvent s'exécuter sur tous types de fichiers numériques pour générer une séquence alphanumérique de longueur fixe qui peut être utilisée pour attester qu'un fichier numérique n'a pas été modifié. Cette séquence restera la même chaque fois que le calcul est exécuté pour autant que le fichier n'ait pas changé.

Informatique en cloud (ou en nuage) (cloud computing) : un modèle d'opérations qui permet le stockage, le traitement et l'analyse de données sur un intranet ou sur Internet. Le cloud (ou nuage) peut être privé, public ou hybride.

Ingénierie sociale (ou piratage psychologique) (social engineering) : la manipulation psychologique d'une personne afin d'obtenir un accès non autorisé à ses informations. Le procédé est similaire au piratage (hacking), à la différence qu'il cible une vulnérabilité humaine plutôt qu'une vulnérabilité technique. L'ingénierie sociale se pratique sous de nombreuses formes différentes, comme l'hameçonnage et le harponnage.

Intelligence artificielle (artificial intelligence (AI)) : une branche de l'informatique consacrée à la programmation de machines capables d'apprendre à réagir à des variables inconnues et à s'adapter à de nouveaux environnements.

Interface de programmation d'applications (API) (application programming interface) : ensemble d'instructions informatiques qui permettent à des logiciels de communiquer entre eux.

Internet Assigned Numbers Authority (IANA) : l'organisme qui supervise l'attribution mondiale des adresses IP, des numéros de systèmes autonomes et des systèmes de noms de domaine.

Intranet : un réseau informatique privé qui utilise les protocoles d'Internet et la connectivité en réseau pour créer une version locale d'Internet.

Langage de balisage hypertexte (ou langage hypertexte) (HTML) : un langage de programmation qui est utilisé pour concevoir les pages Web accessibles par l'intermédiaire d'un navigateur.

Logiciel d'analyse prédictive (predictive software) : logiciel qui utilise des algorithmes prédictifs et l'apprentissage automatique pour analyser les données et faire des prédictions concernant l'avenir ou des faits et comportements inconnus.

Logiciel malveillant (malware) : logiciel conçu pour porter préjudice à un appareil numérique, un réseau, un serveur ou un utilisateur. Il existe de nombreux types différents de logiciels malveillants, parmi lesquels les virus, les chevaux de Troie, les

rançongiciels ou logiciels rançonneurs, les publiciels ou logiciels publicitaires, et les logiciels espions ou mouchards ou spyware.

Machine virtuelle (virtual machine) : logiciel qui imite un système informatique.

Mégadonnées (big data) : grands ensembles de données qui peuvent être analysés pour détecter des corrélations entre points de données et révéler des schémas qui peuvent servir aux capacités prédictives. Les principales caractéristiques des mégadonnées sont leur volume et leur complexité.

Métadonnées (metadata) : ce sont des données au sujet des données. Elles contiennent des informations concernant les fichiers électroniques, qui sont intégrées ou associées à ceux-ci. Elles contiennent souvent les caractéristiques d'un fichier et son historique, notamment son nom, sa taille, les dates auxquelles il a été créé et modifié, et par qui il a été collecté, créé, consulté, modifié et formaté.

Nom de domaine (domain name) : étiquette qui identifie un domaine de réseau. Sur Internet, les noms de domaine sont formés selon les règles et les procédures du système de noms de domaine (DNS). En général, le nom de domaine représente une ressource du protocole Internet (IP), comme l'ordinateur personnel utilisé pour accéder à Internet, le serveur hébergeant un site Web, le site Web lui-même, ou tout autre service communiqué via Internet.

Pixel espion (ou pixel invisible) (beacon) : un mécanisme qui suit l'activité et le comportement de l'utilisateur. Les pixels espions sont faits d'un petit élément peu voyant (souvent invisible) inséré dans une page Web (aussi petit qu'un seul pixel transparent) qui, lorsqu'il est affiché par le navigateur communique à des tiers des détails concernant le navigateur et l'ordinateur utilisés.

Prospection en données (ou data mining) : la pratique consistant à examiner et à extraire des données de bases de données afin de générer des connaissances ou de nouvelles informations.

Protocole de transfert hypertexte (HTTP) : le protocole qui sous-tend Internet et qui définit comment les données sont transférées et reçues.

Pseudonymisation (pseudonymization) : le traitement des données personnelles de telle sorte que les informations concernées ne puissent plus être attribuées à la personne sans un complément d'informations.

Ratissage (ou scraping) : procédé consistant à extraire des quantités massives de données des sites Web.

Recherche booléenne (Boolean search) : une technique de recherche sur Internet qui permet aux utilisateurs de combiner des mots clefs avec des opérateurs ou modificateurs (ET, SANS, OU) pour affiner la recherche et obtenir des résultats plus pertinents et ciblés.

Réseau local (LAN) : une collection d'appareils numériques connectés au même réseau dans un lieu physique défini.

Réseau privé virtuel (VPN) : un réseau ou système sécurisé constitué de nœuds sûrs qui recourent au cryptage et à d'autres dispositifs de sécurité pour veiller à ce que seuls les utilisateurs autorisés puissent accéder au réseau. Les VPN masquent l'adresse IP et protègent les données de l'interception.

Salon de discussion (chat room) : un site Web sur Internet qui permet aux utilisateurs d'avoir une conversation en ligne en temps réel.

Signature cryptographique (cryptographic signature) : un processus mathématique pour vérifier l'authenticité d'un élément numérique. En recourant à un algorithme, on peut générer deux clefs mathématiquement liées : l'une privée et l'autre publique. Un logiciel est utilisé pour créer un hachage des données électroniques. La clef privée est alors utilisée pour crypter le hachage.

Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) : la société chargée de veiller au fonctionnement stable et sûr d'Internet en coordonnant l'administration et les procédures de plusieurs bases de données relatives aux espaces des noms et des nombres sur Internet.

Stripping : un processus technologique pour supprimer les métadonnées d'un fichier sans le convertir en d'autres formats.

Système de noms de domaine (DNS) : le système par lequel est réglementée l'attribution des noms de domaine.

Titulaire de nom de domaine (domain name registrant) : la personne, la société ou l'entité qui détient les droits d'un nom de domaine.

Traqueur (tracker) : un type de cookie qui exploite la faculté d'un navigateur de garder une trace des pages Web visitées, des critères de recherche saisis, etc. Les traqueurs sont généralement des cookies permanents qui tiennent un registre continu du comportement d'un visiteur donné.

Web (WWW) : un espace d'information dans lequel les documents et les autres ressources sont identifiés par des URL, peuvent être reliés entre eux par des hyperliens et sont accessibles sur Internet. Les ressources du Web sont consultables par les utilisateurs au moyen d'une application appelée navigateur.

Web visible (surface Web) : la partie d'Internet qui peut être consultée par tout navigateur et interrogée au moyen des moteurs de recherche traditionnels.

WHOIS : annuaire qui fournit l'identité du propriétaire d'un nom de domaine sur la base de l'entité qui a procédé à son enregistrement. Les enquêteurs en sources ouvertes pourraient utiliser un outil de recherche dans WHOIS dans le cadre de leur processus d'analyse et de vérification des sources.

ANNEXES

SOMMAIRE

- Modèle de plan d'enquête en ligne
- Modèle d'évaluation des menaces et des risques numériques
- Modèle d'état des lieux du paysage numérique
- Formulaire de collecte de données en ligne
- Considérations pour la validation de nouveaux outils

Annexe I

Modèle de plan d'enquête en ligne

Numéro de référence de l'enquête :	
Date de l'évaluation :	
Résumé de l'enquête : *matière et portée territoriale et temporelle de l'enquête*	

1. Objectifs et activités prévues

Objectifs et stratégie de l'enquête en ligne, activités précises assorties d'un calendrier d'exécution.

2. Résumé de l'état des lieux du paysage numérique

État des lieux du paysage numérique dans le territoire géographique sous enquête, notamment les médias sociaux populaires, les applications mobiles et autres technologies présentes, les personnes qui ont accès à ces services et les personnes qui les utilisent.

3. Stratégie d'atténuation des risques et mesures de protection

Principales constatations et conclusions de l'évaluation des menaces et des risques numériques ; stratégie de détection, de gestion et de riposte face aux menaces relevées.

4. Cartographie des acteurs

Intervenants de première ligne (qui pourraient avoir collecté en ligne des contenus potentiellement pertinents disparus depuis) ; fournisseurs d'archives numériques, d'accès à Internet et de services sur le Web (qui pourraient avoir des versions originales ou des métadonnées supplémentaires relatives à des contenus en ligne qui sont disponibles sur simple demande d'assistance). Bien que les enquêteurs non judiciaires pourraient ne pas être légalement habilités à demander des informations de sources fermées, l'assistance de contacts auprès des fournisseurs d'accès à Internet pourrait s'avérer précieuse pour obtenir des réponses à certaines questions et une aide à la navigation de leurs plateformes.

5. Rôles et responsabilités

Rôles et responsabilités des membres de l'équipe, avec désignation d'une personne chargée de coordonner les activités en ligne. La question de savoir qui pourrait déposer en justice, le cas échéant, pourrait également être envisagée.

6. Ressources

Évaluation des besoins en personnel (nombre d'enquêteurs, diversité et inclusivité de l'équipe) et des besoins éventuels en formation spécialisée et en équipement pour mener à bien les activités d'enquête en ligne.

7. Consignation

Directives précises aux membres de l'équipe quant à la consignation de leurs activités d'enquête en ligne (comment, où).

Annexe II

Modèle d'évaluation des menaces et des risques numériques

Numéro de référence de l'enquête :	
Date de l'évaluation :	
Résumé de l'enquête : *matière et portée territoriale et temporelle de l'enquête*	
Objectifs de l'enquête :	

1. Quels sont vos actifs ?

Personnes (ventilées par genre) :

Actifs corporels :

Actifs incorporels (données, etc.) :

2. Quelles sont vos vulnérabilités ?

3. Quelles menaces pourraient cibler ces vulnérabilités et porter préjudice à vos actifs ?

4. Qui sont les auteurs susceptibles de mettre ces menaces à exécution ?

A. Quels sont leurs intérêts ?

B. Quelles sont leurs capacités ?

C. Quelle est la probabilité d'une attaque ?

5. Quelles mesures d'atténuation des risques sont possibles et souhaitables ? Y a-t-il des risques genrés dont il faut tenir compte ?

Considérer les aspects suivants :

- Préjudices physiques
- Préjudices numériques
- Préjudices psychosociaux

Annexe III

Modèle d'état des lieux du paysage numérique

Numéro de référence de l'enquête :	
Date de l'évaluation :	
Résumé de l'enquête : *matière et portée territoriale et temporelle de l'enquête*	
Objectifs de l'enquête :	

L'astérisque (*) indique que les enquêteurs devraient prendre en compte divers facteurs comme l'âge, le genre, le lieu et d'autres informations démographiques pertinentes.

1.	Parties concernées (communautés, groupes armés, etc.). Pour chaque partie, indiquer les différences d'usage de la technologie ou de présence en ligne selon le genre, l'âge ou le handicap.
2.	Langues concernées (y compris l'argot et d'autres langues d'initiés)*
3.	Usage fréquent des moteurs de recherche*
4.	Plateformes de médias sociaux populaires*
5.	Sites Web populaires*
6.	Usage/pénétration d'Internet (ventilation par genre, âge, etc.)
7.	Préférences en matière de téléphonie mobile/système d'exploitation (ventilation par genre, âge, etc.)
8.	Applications mobiles populaires (ventilation par genre, âge, etc.)
9.	Fournisseurs de services de télécommunication
10.	Connectivité : emplacements Wi-Fi/tours cellulaires
11.	Législation concernée (liberté d'expression, accès à l'information, vie privée)
12.	Organes de presse et reporters (présence en ligne)
13.	Bases de données ouvertes (par exemple, données des pouvoirs publics, des ONG, des chercheurs)
14.	Bases de données payantes (par exemple, données des pouvoirs publics, des sociétés privées, des chercheurs)
15.	Représentativité des contenus en ligne (groupes inclus contre groupes exclus)

Annexe IV

Formulaire de collecte de données en ligne

1. Renseignements relatifs à la personne chargée de la collecte

Enquête :

Collecteur ou collectrice :

Adresse IP du collecteur ou de la collectrice :

Début de la collecte (date/estampille temporelle) :

Fin de la collecte (date/estampille temporelle) :

2. Informations visées

Adresse Web (URL) :

Code source HTML :

Capture d'écran :

Données saisies :

Adresse(s) IP :

3. Renseignements relatifs au lot collecté

Nom du fichier du lot collecté :

Liste de hachage du lot collecté :

Hachage du fichier de la liste de hachage du lot collecté :

4. Services utilisés

Produit(s) logiciel(s) :

Service temps :

Service IP :

Service WHOIS :

Annexe V

Considérations pour la validation de nouveaux outils

Caractéristiques

- Code source ouvert contre code source fermé
- Payant contre libre
- Identité, affiliations ou intérêts du propriétaire (individu ou société)
- Financement (Comment et dans quelle mesure l'outil est-il financé ? Quelle est la durée de vie probable du produit ?)

Questions de sécurité

- À qui appartient l'outil ou le code sous-jacent ?
- Le code sous-jacent est-il de source ouverte ou fermée ?
- L'outil est-il soumis à un contrôle indépendant ?
- Où les données collectées seront-elles stockées ?
- Qui aura accès aux données collectées ?
- Quelle est l'infrastructure de sécurité de l'outil ?
- Quelles obligations légales pourraient affecter la sécurité d'utilisation de l'outil ?
- En cas de violation de la loi, y a-t-il un droit de recours ?

Questions opérationnelles

- L'outil est-il fonctionnel ?
- L'outil est-il facile à utiliser ?
- Quelles sont les capacités de soutien aux utilisateurs du propriétaire, du fournisseur ou de l'outil ?
- Quelle est la fréquence de mise à jour de l'outil ?
- Quelle est la compatibilité de l'outil avec d'autres systèmes ?

HUMAN RIGHTS CENTER
UC Berkeley School of Law

University of California
Human Rights Center (HRC)
2224 Piedmont Avenue
Berkeley, CA 94720
Courriel : hrc@berkeley.edu
Site Web : https://humanrights.berkeley.edu/

NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

Haut-Commissariat des Nations Unies
aux droits de l'homme
Palais des Nations
CH 1211 Genève 10, Suisse
Courriel : ohchr-infodesk@un.org
Site Web : www.ohchr.org/fr

Copublié par les Nations Unies, pour le compte du Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH), et le Human Rights Center de la faculté de droit de l'Université de Californie à Berkeley.

ISBN: 978-92-1-154245-5

Printed at United Nations, Geneva – 2012695 **(F)** – January 2024 – 1,595 – **HR/PUB/20/2**