DPPC

Droit Pénal et Politique Criminelle
Derecho Penal y Política Criminal

La recherche et l'administration de preuves numériques liées à la propagande terroriste: l'exemple d'une police cantonale en Suisse

Robin Kjelsson

Proposition de citation: Robin Kjelsson, La recherche et l'administration de preuves numériques liées à la propagande terroriste: l'exemple d'une police cantonale en Suisse, in: Revue DPPC, 2025, Volume 1, pp. 64-90.

URL: <https://www.dppc.online>

Résumé

Cet article analyse, dans une perspective pratique, les enjeux et les difficultés liés à la recherche, à la saisie et à la conservation des preuves numériques dans le cadre d'une procédure pénale relative à la propagande terroriste. Il expose d'abord les considérations procédurales issues du Code de procédure pénale suisse, qui définissent le champ d'action de la police avant et durant l'enquête pénale. S'appuyant ensuite sur l'expérience professionnelle de l'auteur en tant que gendarme à la police cantonale neuchâteloise, sur une interview de spécialistes de l'investigation numérique et sur des directives internes de la police neuchâteloise, la contribution consacre sa partie principale à l'examen des aspects techniques de la collecte des preuves numériques.

Resumen

Este artículo analiza, desde una perspectiva práctica, los retos y dificultades que plantea la búsqueda, la incautación y la conservación de pruebas digitales en el marco de un proceso penal relacionado con la propaganda terrorista. En primer lugar, expone las consideraciones procesales derivadas del Código de Procedimiento Penal suizo, que delimitan el ámbito de actuación policial antes y durante la investigación penal. Posteriormente, basándose en la experiencia profesional del autor como agente de la policía cantonal de Neuchâtel, en una entrevista con especialistas en investigación digital y en directrices internas de dicha institución, la contribución dedica su parte principal al examen de los aspectos técnicos de la recolección de pruebas digitales.

Abstract

This article analyses, from a practical perspective, the challenges and difficulties associated with the search, seizure, and preservation of digital evidence in criminal proceedings related to terrorist propaganda. It first outlines the procedural considerations derived from the Swiss Criminal Procedure Code, which define the scope of police action before and during the investigation. Building on the author's professional experience as a gendarme with the Neuchâtel cantonal police, on an interview with specialists in digital forensics, and on internal guidelines issued by that institution, the main part of the contribution focuses on the technical aspects of collecting digital evidence.

Sommaire

Introduction	67
Méthodologie	69
I. La recherche des preuves numériques	69
A. Généralités	69
B. Bases légales et compétences	70
1. Avant l'introduction de la procédure pénale	71
2. Pendant la procédure pénale	73
C. Méthodes de recherche	77
1. Détection	77
2. Identification de l'auteur	79
D. Méthodes de saisie	80
1. Protocoles	82
2. Dangers	83
II. Les problématiques liées à l'administration des preuves	84
A. Authentification	84
B. Chaîne de conservation et sauvegarde à des fins judiciaires	86
Conclusion	87
Bibliographie	88

Introduction

[1] Même si, dernièrement et sur son territoire, la Suisse semble relativement épargnée par les actes terroristes – les rares évènements ayant marqué l'opinion publique étant les attaques au couteau de Morges et de Lugano en 2020 et de Zurich en 2024 – en comparaison internationale, le danger d'attentats subsiste aux yeux des autorités¹. Le **terrorisme**² ne connaît pas de frontières territoriales: outre les actes matériels ponctuels perpétrés dans le monde physique, une autre réalité les a définitivement effacées, celle du monde numérique. Si celui-ci en a entre autres facilité le financement (réprimé notamment par les art. 260^{quinquies} et 260^{sexies} al. 2 du Code pénal suisse, ci-après CP), via les cryptomonnaies par exemple, nous laisserons de côté cet aspect dans la présente contribution³ pour considérer son usage dans le contexte de la propagande terroriste.

[2] Par **propagande**, on entend au sens juridique suisse du terme n'importe quel acte (objectivement) perceptible par d'autres, y compris le simple geste, dans la conscience et l'intention (subjectives) que cet acte sera perçu comme de la publicité, c'est-à-dire d'agir sur les autres de telle sorte qu'ils soient gagnés aux idées exprimées ou, s'ils y ont déjà adhéré, qu'ils soient confortés dans leurs convictions⁴. En d'autres termes, il s'agit de répandre une idée en faisant de la publicité⁵ pour rallier un destinataire à sa conviction ou le conforter dans son opinion préexistante⁶, peu importe le vecteur.

[3] Dans ce contexte, les possibilités du numérique visant l'apologie du terrorisme ont explosé, sans mauvais jeu de mot, par l'usage des réseaux sociaux. À tel point que ceux-ci sont devenus le véhicule privilégié des terroristes⁷, permettant de diffuser leur propagande auprès de millions de personnes en un instant. On peut aller jusqu'à parler de *cyberterrorisme*⁸.

[4] Les **infractions** réprimant la propagande numérique terroriste en droit pénal suisse sont principalement: la participation ou le soutien à une organisation terroriste (art. 260^{ter} CP)⁹; son

---

¹ Voir également: HEIMGARTNER / INHELDER, p. 1217.

² Il en existe probablement autant de définitions que d'auteurs différents et d'éclairages possibles (juridique, historique, sociologique, militaire, politique, etc.). Nous nous bornerons dans la présente contribution à définir le terrorisme en référence à l'article 260^{quinquies} CP comme « *un acte de violence criminelle visant à intimider une population ou à contraindre un Etat ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque* ». Voir également: [FF 2018 6469](#), p. 6514; [ATF 146 IV 338](#) c. 4.4.2; AJIL / LUBISHTANI, p. 22; LAUBER / MEDVED, p. 191.

³ Certaines réflexions développées ci-dessous pourront toutefois y être appliquées *mutatis mutandis*.

⁴ [ATF 140 IV 102](#) c. 2.2.2; [ATF 68 IV 145](#) c. 2; [arrêt du TPF SK.2017.49](#) c. 2.2.3.2. Voir également: HEIMGARTNER / INHELDER, p. 1224.

⁵ La publicité et la propagande ne se distinguent que par leur champ d'application (commercial pour la première, idéologique, politique ou religieux pour la seconde): [arrêt du TPF SK.2022.57](#) c. 3.3.6.

⁶ [ATF 150 IV 10](#) c. 5.2.2.

⁷ [Arrêt du TPF SK.2007.4](#) c. 4.2.3; AJIL / LUBISHTANI, p. 38; CEP, *Extremist Content*, p. 1; LAUBER, p. 194; LEU / PARVEX, p. 762; MOREILLON / LUBISHTANI, p. 539.

⁸ [Arrêt du TF 6B 645/2007](#) c. 7.2.3.

⁹ En témoignent les nombreux jugements fédéraux: arrêt du TF [6B 1104/2016](#); [SK.2019.23](#). Pour un aperçu jurisprudentiel, voir: HEIMGARTNER / INHELDER, p. 1230 et AJIL / LUBISHTANI, p. 23 ss.

pendant sur l'encouragement à ses activités (art. 74 al 4 LRens)¹⁰; le recrutement d'adeptes (art. 260^{sexies} CP)¹¹; et la représentation de la violence (art. 135 al. 1 CP)¹². Toutes ces dispositions permettent par exemple de sanctionner la mise à disposition sur Internet de forums de discussion terroristes ou la diffusion de messages sur ces plateformes¹³, la diffusion de contenu terroriste sur des réseaux sociaux comme Youtube, Google+ ou Facebook¹⁴, l'échange de messages via WhatsApp, Telegram et Facebook Messenger¹⁵, et le téléchargement depuis l'Internet de contenu terroriste violent¹⁶. Faute de propagande active mais si un message sur un forum appelle à tuer des otages par exemple, ce comportement peut être constitutif de provocation publique au crime ou à la violence (art. 259 CP)¹⁷. Enfin, on citera encore que si la propagande terroriste n'est pas suffisante pour être qualifiée de soutien à un groupe terroriste, le fait de propager une idéologie haineuse vis-à-vis d'un groupe de personnes est incriminé par la discrimination et l'incitation à la haine (art. 261^{bis} CP)¹⁸.

[5] Pour punir pénalement cette propagande terroriste, sans parler de la prévenir ou de la surveiller, les autorités pénales ont besoin de preuves. Or, qui dit usage de l'Internet ou de supports informatiques, dit preuves numériques. À la différence des preuves matérielles et de par leur nature, les **preuves numériques** posent des défis considérables en matière de recherche, de saisie et de préservation en vue de leur exploitation dans un procès pénal. De quoi rendre la tâche encore plus délicate qu'elle ne l'était avant l'avènement de l'ère digitale aux principaux acteurs de leur récolte, à savoir les services de police. Ceux-ci se sont adaptés en créant davantage de moyens pour combattre la cybercriminalité, notamment par l'embauche de spécialistes forensiques en informatique et en analyse.

[6] C'est donc dans cette optique que la présente contribution propose, modestement, d'offrir au lecteur juriste un éclairage technique et pratique d'enquêteurs professionnels de la **police neuchâteloise** (ci-après: abrégée PONE) sur la **récolte des preuves numériques**, dans le cadre de la propagande terroriste. L'auteur et soussigné travaille en effet à la gendarmerie de la police neuchâteloise.

---

¹⁰ Rappelons que cet article a remplacé l'ancienne [Loi fédérale interdisant les groupes « Al-Qaïda » et « Etat islamique » et les organisations apparentées du 12 décembre 2014](#) (LAQEI), promulguée dans l'urgence et temporaire (jusqu'au 31 décembre 2022), qui réprimait à son art. 2 l'association, le soutien, la propagande et le recrutement au profit des groupes terroristes. Voir: AJIL / LUBISHTANI, p. 29; LEU / PARVEX, p. 756.

¹¹ [Arrêt du TF 7B 87/2022](#).

¹² Particulièrement dans le domaine digital, l'al. 1^{bis} sanctionne l'acquisition, l'obtention ou la possession de tels contenus par voie électronique ou d'une autre manière, permettant par cette formulation d'inclure des formes de mémoire de données ou des moyens de transmission (électroniques) non encore actuels. Voir: [arrêt du TPF SK.2007.4](#) c. 6.2.7; HAGENSTEIN, art. 135 CP n° 64.

¹³ [Arrêt du TF 6B 645/2007](#) c. 7.3; [arrêts du TPF SK.2019.23](#) c. 4 et [SK.2007.4](#) c. 4.3 (avec références); AJIL / LUBISHTANI, p. 27; WOHLERS, art. 260^{ter} CP n° 8; MOREILLON / LUBISHTANI, p. 542; PAJAROLA, p. 94.

¹⁴ LAUBER / MEDVED, p. 189.

¹⁵ Même de manière non publique mais adressée à un cercle fermé de personnes, voire à une seule: [arrêt du TPF SK.2017.39](#).

¹⁶ [Arrêt du TPF SK.2007.4](#) c. 6.2.7.

¹⁷ [Arrêt du TF 6B 645/2007](#) c. 7.2.3.

¹⁸ Rapport du CF, [Extrémisme](#), p. 4; [ATF 150 IV 10](#) c. 5.2.2.

Méthodologie

[7] À l'instar des nombreux autres domaines d'action de la police (usage de l'arme, comportement en cas d'accident, par exemple), ceux de la perquisition, de la saisie et de la conservation des preuves numériques ainsi que des recherches anonymes sur Internet a fait l'objet de **directives internes** à la PONE, édictées par sa direction ou par les chefs des entités de police judiciaire. Ces circulaires, basées sur le CPP ainsi que sur la Loi neuchâteloise sur la police¹⁹ (ci-après: LPol-NE) pour l'aspect légal, rappellent tout d'abord les limites à l'action policière. Bien plus cependant, et c'est là leur utilité principale, elles offrent pour l'aspect matériel des conseils, des comportements prescrits et des bonnes pratiques à adopter afin d'assurer au mieux le succès de la procédure pénale (préliminaire) mise en œuvre par la police, pour que soient transmises les preuves, sous forme sauvegardée et apte à l'usage judiciaire, au ministère public ou aux tribunaux, les destinataires finaux du fruit de dur labeur des techniciens.

[8] Le présent article se base donc, outre sur les références de la jurisprudence et la doctrine citées, sur les circulaires (ci-après: circ.) pertinentes édictées par la PONE en matière de preuves numériques. Par souci d'économie d'espace, elles ne seront pas reproduites ici; cependant, bien que n'étant pas accessibles librement sur Internet, leur contenu n'est pas secret et sera transmis à n'importe qui en fera la demande à sa direction (ce qui a déjà été le cas pour des journalistes, par exemple). Nous nous bornerons ici à citer le nom de la directive en question.

[9] Enfin, les techniques de saisie, de recherche et de conservation des preuves numériques sont largement affaire de spécialistes du domaine, dont les expériences acquises par la pratique seront toujours, de notre humble avis, infiniment plus riches que tout mode d'emploi. Dès lors et à l'occasion de cette contribution, deux spécialistes de l'Investigation Numérique (abrégée IN ci-après) de la PONE ont été interviewés, sur une série de questions en rapport avec la thématique. Désirant rester anonymes, ces collègues du soussigné ne seront pas cités, et leur contribution figure telle quelle dans le texte, sans référence.

I. La recherche des preuves numériques

A. Généralités

[10] Nous entendons par « **preuves numériques** », au sens forensique du terme, les traces consécutives à un événement²⁰ qui permettent d'en détecter la survenance dans un but d'investigation judiciaire, ici sous la forme de **données** en format informatique²¹. Au sens légal du terme, on rappellera qu'une preuve peut constituer en n'importe quel élément propre à établir la vérité, dénotant par-là une définition large incluant les données numériques, et une absence de *numerus clausus* des moyens (art. 139 CPP). Ainsi, les données comprennent simplement (et de façon certes un peu tautologique) toute information susceptible d'être utilisée comme moyen de preuve²².

---

¹⁹ [RS-NE 561.1](#).

²⁰ JAQUET-CHIFFELLE, p. 2, qui emploie les termes « preuve » et « trace » comme synonymes.

²¹ JAQUET-CHIFFELLE, p. 199; LUDWICZAK GLASSEY, p. 118.

²² BENHAMOU / OETTLI, p. 209 et réf. citées. La police n'utilise pas de définition technique particulière.

[11] Une donnée peut être numérique **par nature** (fichier sur un ordinateur, contenu d'une page Internet, enregistrements sur un serveur) ou résulter d'une **numérisation** d'un événement matériel (photographie ou vidéo d'une chose ou d'un acte, enregistrement d'une voix)²³. En termes numériques, LUDWICZAK GLASSEY distingue les données relatives aux abonnés (« qui » en est la cause), au trafic (ou *métadonnées*, « comment » elles sont générées) et au contenu (« quoi » est l'information elle-même)²⁴.

[12] On trouvera les preuves numériques sur des **supports physiques** (disque dur, ordinateur, clef USB, CD-Rom, *smartphone*, appareil GPS, etc.) ou des serveurs physiques stockant leur **source incorporelle** (l'Internet, comprenant pages web, Darkweb, moteurs de recherche, *clouds*, e-mails et comptes de messagerie, forums, chats, réseaux sociaux, applications, blockchains, etc.)²⁵.

B. Bases légales et compétences

[13] Comme l'énonce l'article 24 al. 1 CPP, les principales infractions regardant le terrorisme fondent la **compétence juridictionnelle fédérale** si les actes ont été commis pour une part prépondérante à l'étranger (lit. a), ou dans plusieurs cantons sans prédominance évidente dans l'un d'eux (lit. b)²⁶. La doctrine et la jurisprudence ont élargi la compétence fédérale en oblitérant ces deux conditions, englobant également le soutien aux organisations terroristes depuis la Suisse²⁷ et peu importe si l'auteur a agi dans un seul canton: les autorités fédérales sont plus spécialisées dans ce domaine, au contraire des autorités cantonales qui n'y sont peu ou pas confrontées²⁸. Avec PAJAROLA²⁹, nous critiquons cet argument dans la mesure où il n'est pas démontré en pratique de réelle déficience des cantons par rapport à la Confédération dans la lutte contre le terrorisme: ceux-ci disposent pour certains d'unités spécialisées et de davantage de personnel, permettant également un réseau international; de plus, leur connaissance accrue de la situation locale (intra-cantonale), notamment par leurs réseaux avec d'autres services étatiques et le contact « *de près* » avec de potentiels terroristes, reste un atout.

[14] Dans la mesure où les **autorités cantonales** (et donc ici la PONE) ont la compétence de mener les premières investigations selon certaines conditions de l'art. 27 CPP³⁰, et puisque la technique de récolte des preuves numériques ne diffère pas entre Confédération et cantons, ce point n'aura pas d'incidence sur la suite, partant, il ne sera pas approfondi plus avant³¹. De plus,

²³ JAQUET-CHIFFELLE, p. 199; POLLITT et al., p. 2, nos exemples.

²⁴ LUDWICZAK GLASSEY, p. 118 s.

²⁵ Pour des descriptions plus précises de ces éléments, voir: TIRELLI.

²⁶ AJIL / LUBISHTANI, p. 5; LAUBER / MEDVED, p. 186.

²⁷ [Arrêt du TPF SK.2007.4](#) c. 1.1.3; BOUVERAT, art. 24 CPP n° 5.

²⁸ [Arrêt du TPF BG.2018.57](#) c. 2.7; JOST / NIGGLI, art. 24 CPP n° 3 ss; BOUVERAT, art. 24 CPP n° 3; LAUBER / MEDVED, p. 190.

²⁹ PAJAROLA, p. 235 à 241.

³⁰ LAUBER / MEDVED, p. 190.

³¹ Pour un aperçu historique, téléologique et pratique, voir; [arrêt du TPF BG.2018.57](#) c. 2. Pour un argumentaire détaillé, voir: PAJAROLA, p. 236 à 245.

on notera que la lutte au sens large contre le terrorisme implique bien évidemment les cantons et les communes, dont la collaboration est capitale dans la phase préventive de détection³².

1. Avant l'introduction de la procédure pénale

[15] Pour prévenir la propagande terroriste sur Internet, des outils existent en amont de la procédure pénale. Nous en esquissons brièvement certains, dans la mesure où ils touchent à la compétence ou à l'activité de la police³³ et soulèvent également des difficultés liées à l'aspect numérique.

[16] Depuis le 1^{er} juin 2022 sont entrées en vigueur les dispositions de la Loi sur les **mesures policières de lutte contre le terrorisme** (MPT), non sous la forme d'une loi unique mais d'ajouts ou de modifications de dispositions d'autres lois fédérales, parmi elles la LMSI (particulièrement les art. 23^e à 23^r LMSI, dont seul l'art. 23^q LMSI est de nature numérique) et la LSCPT (art. 1 et 11 LSCPT, voir ci-dessous). Elles visent à renforcer les mesures policières existantes en dehors d'une procédure pénale³⁴, possiblement avec l'usage de mesures de contrainte³⁵.

[17] La LMSI permet, à son article 13^e al. 1, aux autorités policières (fédérales) de saisir tout « matériel qui peut servir à des fins de propagande et dont le contenu incite, d'une manière concrète et sérieuse, à faire usage de la violence contre des personnes ou des objets », également en cas de soupçon (al. 4). La diffusion par le biais d'Internet est également prise en compte, de manière limitée, à l'al. 5: il permet la suppression de contenu si le serveur est situé en Suisse (lit. a), la révocation des noms de domaine dont la gestion relève de la compétence de la Suisse (lit. a^{bis}) ou la recommandation au fournisseur suisse de bloquer le site si ses serveurs sont situés à l'étranger (lit. b). Enfin, la surveillance électronique et la localisation par téléphonie mobile (art. 23^q LMSI) concerne en réalité le terroriste potentiel (art. 23^e al. 1 LMSI) et non tout auteur de propagande, et se limite à l'obliger à porter sur lui un appareil localisable³⁶.

[18] La LMSI étant limitée à cause de son art. 14 al. 3 (« le recours à des mesures de contrainte prévues par la procédure pénale n'est permis que dans le cadre d'une procédure d'enquête de police judiciaire ou d'une instruction préparatoire. Il en va de même de l'observation de faits dans des locaux privés »), la collecte préventive d'informations sur Internet se base plutôt sur la **LRens, qui a remplacé la LMSI**³⁷. On notera également que la LMSI évoque une seule disposition pénale (art. 29^a LMSI, un délit sanctionnant le non-respect des mesures visées aux art. 23^l à 23^q LMSI et une contravention sanctionnant la violation de l'art. 23^k LMSI), qui n'est pas comprise dans le catalogue d'infractions de l'art. 269 al. 2 CPP permettant une surveillance de la télécommunication.

³² LAUBER / MEDVED, p. 184 évoquant le programme TETRA (TERRORIST TRACKING) de Fedpol. Voir également: Rapport du CF, *Extrémisme*, p. 10; [FF 2019 4541](#), p. 4554 et 4556; [FF 2018 6469](#), p. 6506.

³³ Toutefois avec retenue dans le domaine préventif: AJIL / LUBISHTANI, p. 4 et 40.

³⁴ [FF 2019 4541](#), p. 4542.

³⁵ LAUBER / MEDVED, p. 194. Pour une analyse approfondie, voir: LUBISHTANI / MONOD (constitutionnalité douteuse); AJIL / LUBISHTANI, p. 40 ss (dualité floue entre droit pénal et administratif); MOREILLON / LUBISHTANI, p. 546 (idem).

³⁶ LAUBER / MEDVED, p. 193.

³⁷ D'AVILA BENDAYA, p. 202, 204, 211. Voir également: PLATZ, pt III.3: les art. 14^a à 18^a LMSI ont été abrogés au profit de la LRens.

[19] Dans le contexte préventif de détection de propagande terroriste numérique, l'utilisation de moyens de surveillance et de perquisition secrète est fournie par la **LRens**³⁸. De manière générale, ses mesures sont soumises à autorisation (du chef du Département fédéral de la défense, de la protection de la population et des sports, finalement du Tribunal administratif fédéral, sauf pour les recherches OSINF soient les informations publiques: art. 13 ss LRens), et concernent les menaces en matière de sécurité sans lien nécessaire avec une procédure pénale³⁹. À ce titre, on citera les mesures de l'art. 26 LRens permettant de surveiller la correspondance par télécommunication et d'utiliser à cette fin des appareils techniques, pour géolocaliser ou écouter des propos privés, ou encore pour s'infiltrer dans des systèmes et réseaux informatiques⁴⁰. Ces mesures sont exécutées secrètement (art. 26 al. 2 LRens).

[20] Dans le contexte international du risque terroriste, l'**art. 37 LRens** permet au SRC d'infiltrer des systèmes et réseaux informatiques situés à l'étranger⁴¹, afin de perturber, empêcher ou ralentir l'accès aux informations. Enfin, l'**art. 39 LRens** permet également l'exploration du réseau câblé sur les signaux circulant en Suisse: il s'agit d'intercepter les communications internationales par le biais d'Internet, en donnant l'accès aux métadonnées et contenus des communications telles que les emails, discussions Whatsapp et réseaux sociaux. On précisera que cette surveillance n'est pas ciblée⁴².

[21] Au **niveau cantonal**, l'art. 9 LRens oblige les cantons à désigner une autorité qui collabore avec le SRC et en exécute les mandats dans le cadre de la LRens. Pour le canton de Neuchâtel, il s'agit du Groupe renseignements de la PONE, instauré par l'art. 26a LPol-NE. De même, puisque le CPP ne prévoit plus de surveillance lors de l'enquête préliminaire, celle-ci doit être prévue dans le droit cantonal⁴³. C'est le cas par exemple à Neuchâtel, où les art. 68 ss LPol-NE prévoient la possibilité d'observations préventives (art. 68 LPol-NE), l'utilisation de mesures techniques de surveillance (art. 69 LPol-NE) dans des lieux publics, et autres recherches (art. 70 LPol-NE) et investigations (art. 71 LPol-NE) préliminaires secrètes.

[22] Enfin, on relèvera que ces mesures préventives de surveillance, intervenant certes avant la procédure pénale, sont ciblées et mises en place après la naissance de soupçons dirigés contre une personne ou un utilisateur particulier. Ainsi, il n'existe pas en Suisse de **surveillance générale** et systématique d'Internet⁴⁴. Certaines entités peuvent effectuer une *veille* d'Internet⁴⁵ liée à des infractions précises (principalement la pédopornographie, tout comme la police effectue dans ce cadre une veille proactive⁴⁶), mais leur rôle se limite à signaler aux autorités

³⁸ Rapport du CF, *Extrémisme*, p. 11; MÉTILLE, intro art. 269 à 281 n° 70; D'AVILA BENDAYA, p. 202.

³⁹ D'AVILA BENDAYA, p. 209, 211; HEIMGARTNER / INHELDER, p. 1229; PAJAROLA, p. 282.

⁴⁰ D'AVILA BENDAYA, p. 210 ss.

⁴¹ *Ibid*, p. 221.

⁴² *Ibid*, p. 222 et 223, citant l'arrêt du Tribunal administratif fédéral A-6143/2017 du 4 juin 2019 c. 3.3 pour des détails techniques.

⁴³ PAJAROLA, p. 280 ss, qui relève la frontière floue entre procédure pénale et mesures policières préventives. Voir également: Rapport du CF, *Cybercriminalité*, p. 22.

⁴⁴ COTTIER, p. 691. Notons que l'art. 3 LSCPT (service de surveillance) est lié aux mesures de l'art. 269 CPP et donc à la procédure pénale, pas à une surveillance pré-procédurale.

⁴⁵ *Ibid*, citant le Service national de Coordination de la lutte contre la Criminalité sur Internet (SCOCI), rattaché à Fedpol.

⁴⁶ En plus des signalements transmis par le NCMEC (National Center for missing and exploited children), voir: Rapport du CF, *Cybercriminalité*, p. 4.

compétentes la commission d'une infraction. Enfin, aucune disposition légale n'oblige les fournisseurs de contenus Internet à procéder à une telle veille⁴⁷. Les efforts notamment des plateformes de réseaux sociaux en ce sens sont considérés comme insuffisants⁴⁸.

2. Pendant la procédure pénale

[23] Qu'elle intervienne pendant l'investigation policière (art. 306 ss CPP) ou après l'ouverture de l'instruction par le ministère public (art. 308 ss CPP), la récolte des preuves numériques fait partie des mesures de contrainte⁴⁹, et son objectif est la mise en sûreté des preuves (art. 196 lit. a CPP). Outre le fait qu'elle doit respecter certains principes pour sa mise en œuvre (art. 197 CPP)⁵⁰, la compétence policière est donnée par ordre du ministère public (art. 198 al. 1 lit. a CPP) ou directement par la loi (lit. c)⁵¹.

[24] La principale source d'obtention des preuves numériques reste la **perquisition**⁵²: d'abord pour la saisie de supports numériques présents chez l'auteur ou dans d'autres locaux en Suisse (art. 244 CPP), puis surtout pour l'obtention des données numériques présentes sur lesdits supports. En tant qu'ils *contiennent* les informations numériques, qui ne sont donc pas visibles mais doivent être lues, ils entrent dans la catégorie large⁵³ des **enregistrements** auxquels l'art. 246 CPP s'applique⁵⁴. Le simple fait de fouiller un téléphone, sans en extraire les données, constitue une perquisition⁵⁵. Les données numériques non stockées localement mais sur un serveur distant et accessible depuis la Suisse (messages, comptes de réseaux sociaux, *clouds*) sont également concernées⁵⁶.

[25] À ce propos, on évoquera la problématique des **serveurs situés à l'étranger** et de leur accès par les autorités pénales suisses: en l'état actuel de la législation (CPP, LSCPT) et de la jurisprudence⁵⁷, il n'y a pas d'obligation des fournisseurs de service étrangers de fournir leurs données sur demande directe de l'autorité pénale⁵⁸. Une telle obligation existe uniquement

---

⁴⁷ COTTIER, p. 691.

⁴⁸ CEP, *Extremist Content*, p. 1.

⁴⁹ Même avec l'accord de l'ayant droit en l'absence de contrainte, au demeurant non mentionné dans l'art. 246 CPP: PERRIER DEPEURSINGE, *CPP annoté*, ad art. 246; JEANNERET / KUHN, n° 14023.

⁵⁰ Notamment l'existence de soupçons concrets, la *fishing expedition* étant interdite: THORMANN / BRECHBÜHL, art. 246 CPP n° 7; HOHL-CHIRAZI, art. 246 CPP n° 5; JEANNERET / KUHN, n° 14022 ss.

⁵¹ Par exemple dans l'urgence: THORMANN / BRECHBÜHL, art. 246 CPP n° 11; MOREILLON / PAREIN-REYMOND, art. 246 n° 2; JOSITSCH / SCHMID, art. 246 CPP n° 3.

⁵² *Contra*: PLATZ pt I.1, qui semble reléguer la perquisition « physique » aux méthodes du passé.

⁵³ Afin de tenir compte des progrès technologiques futurs: HOHL-CHIRAZI, art. 246 CPP n° 17; MOREILLON / PAREIN-REYMOND, art. 246 n° 3; JEANNERET / KUHN, n°14020.

⁵⁴ BOMMER / GOLDSCHMID, art. 263 CPP n° 28; HOHL-CHIRAZI, art. 246 CPP n° 18; DONATSCH et al., art. 246 CPP n° 6. Il s'agit des données existant indépendamment d'une télécommunication: concernant ce point, v. plus bas.

⁵⁵ PERRIER DEPEURSINGE, *CPP annoté*, ad art. 246 et réf. citées; MOREILLON / PAREIN-REYMOND, art. 246 CPP n° 11.

⁵⁶ BENHAMOU / OETTLI, p. 212; PERRIER DEPEURSINGE, *CPP annoté*, ad art. 246 CPP; DONATSCH et al., art. 246 CPP n° 8a.

⁵⁷ ATF 143 IV 21 c. 3, *arrêt du TF 1B 142/2016* c. 3.

⁵⁸ L'art. 2 LSCPT (obligation de collaborer) n'y change rien: HOHL-CHIRAZI, art. 246 CPP n° 19.

lorsque le siège du fournisseur se trouve en Suisse, ou lorsqu'il existe une filiale en Suisse et que celle-ci exerce un pouvoir de disposition sur les données⁵⁹. Ainsi et à défaut de consentement volontaire du fournisseur⁶⁰, l'autorité pénale devra passer par l'entraide internationale pour respecter le principe de territorialité, avec les difficultés afférentes: elle présuppose l'identification du lieu de stockage des données, et surtout est d'une lenteur procédurale excessive⁶¹. Toutefois, et dans la mesure où les données en question sont *accessibles* depuis la Suisse, par exemple grâce au mot de passe de l'utilisateur donné, l'absence d'acte de puissance publique à l'étranger en permet la perquisition^{62 63}.

[26] Les informations trouvées dans ces enregistrements étant susceptibles d'être séquestrées (art. 246 *in fine* et 263 CPP), l'ayant droit peut s'opposer au séquestre par la demande d'apposition de **scellés** (art. 248 CPP). Sans entrer dans les détails, nous relèverons que la police (et l'autorité pénale en général) a dès lors l'interdiction d'exploiter ces preuves, et doit le cas échéant demander la levée des scellés (art. 248a CPP) au TMC. Le fait de confier le support à la police, y compris pour un acte purement technique (une copie), est interdit⁶⁴. Toutefois en pratique et dans la majorité des cas, puisque les supports sont prélevés par la police, ils seront conservés dans les locaux de celle-ci après l'apposition de scellés, avec interdiction de les exploiter⁶⁵. Le tri des données scellées afin d'évaluer le bienfondé de sa demande, respectivement de la demande de levée, échoit au juge des scellés: le ministère public n'est (évidemment) pas autorisé à y participer, toutefois les services de police spécialisés (comme l'IN à la PONE) peuvent assister le juge⁶⁶. Dans la pratique, le cas est rarissime.

[27] Les deux types de **séquestre** qui nous intéressent dans le cadre présent sont le séquestre *probatoire* (art. 263 al. 1 lit. a CPP) et le séquestre *conservatoire* (lit. d). Le premier permet de maintenir à disposition de l'autorité les données numériques qui serviront comme preuve lors du procès⁶⁷, puisqu'il peut porter sur des biens de toute nature. Si le cas est simple concernant les supports numériques (ordinateur, disque dur), la question de séquestre **d'une page web** ou d'un site internet est controversée.

---

⁵⁹ BENHAMOU / OETTLI, p. 213; LUDWICZAK GLASSEY, p. 125.

⁶⁰ Prévu par la [Convention de Budapest sur la cybercriminalité, entrée en vigueur pour la Suisse le 1^{er} janvier 2012](#) (RS 0.311.43). Voir: LUDWICZAK GLASSEY, p. 126.

⁶¹ Rapport du CF, [Cybercriminalité](#), p. 20; [ATF 143 IV 21](#) c. 3.2; BENHAMOU / OETTLI, p. 213; THORMANN / BRECHBÜHL, art. 246 CPP n° 4; CARTIER, p. 66; DONATSCH et al., art. 246 CPP n° 9.

⁶² HOHL-CHIRAZI, art. 246 CPP n° 19; DONATSCH et al., art. 246 CPP n° 8a. Ce qui facilite grandement celle-ci: PLATZ pt II.1.

⁶³ Notons qu'il n'est pas possible de forcer l'auteur à fournir ses accès: JOSITSCH / SCHMID, art. 246 CPP n° 2.

⁶⁴ BENHAMOU / OETTLI, p. 220. Cependant, l'autorité peut procéder à l'enregistrement des documents sur une clé USB, pour préserver les preuves (arrêt du TF [7B 515/2024](#) du 3 avril 2025 concernant l'enregistrement de documents bancaires par l'Administration fédérale des contributions).

⁶⁵ Circ. 2.107 A08 de la PONE: Procédure de mise sous scellés, qui mentionne un « lieu sûr ».

⁶⁶ *Ibid*, p. 221. *Contra*: JEANNERET / KUHN, n° 14026e, pour qui l'expert ne peut pas être de la police. Selon nous, puisque les ressources professionnelles et infrastructurelles font souvent défaut à toute autre entité que la police, le recours à ses experts semble nécessaire.

⁶⁷ JULEN BERTHOD, art. 263 CPP n° 5; MOREILLON / PAREIN-REYMOND, art. 246 n° 6.

[28] Outre l'assimilation débattue en doctrine des données web à des objets corporels matériels au sens de l'art. 69 CP⁶⁸, le blocage (pénal) d'une page web n'a pas été tranché en jurisprudence ni dans la loi⁶⁹. Il repose sur une interprétation extensive des dispositions sur le séquestre conservatoire (art. 263 CPP: blocage *préventif*) ou la **confiscation d'objets dangereux** (art. 69 CP: blocage *définitif*), et a fait l'objet de revirements de jurisprudence cantonale⁷⁰. Nous nous limiterons à renvoyer le lecteur à BENHAMOU et à approuver, avec lui, l'interprétation extensive pour justifier le blocage (pénal) de sites web propagandistes, à défaut de loi expresse⁷¹.

[29] Enfin, on notera qu'en cas de saisie de données numériques par perquisition ou séquestre, le détenteur des données a la possibilité de remettre aux autorités une **copie** des enregistrements, laquelle devrait suffire aux besoins de la procédure (art. 247 al. 3 CPP). Pour ce faire, elle devrait être une reproduction exacte du support informatique, en incluant par exemple les métadonnées nécessaires à incriminer l'auteur⁷². Dans le cadre de la propagande terroriste numérique toutefois et dans la pratique, c'est la police qui effectuera une copie des données, et le support de l'auteur ou ses données seront vraisemblablement détruites, respectivement bloquées⁷³.

[30] Surtout dans le cadre numérique (emails, messages Whatsapp et Telegram, etc.), le séquestre est à distinguer de la **surveillance par télécommunication** des art. 269 ss CPP: d'une part et vu sa mise en œuvre à l'insu du prévenu, elle obéit à un régime spécial protégé par le secret⁷⁴ et n'est appliquée qu'en *ultima ratio*; d'autre part, elle intervient lorsque la transmission des messages et emails est en cours et que ceux-ci n'ont pas encore été « lus » par l'auteur. Dans ce cas en effet, les données ne sont pas protégées par le secret et donc la perquisition (art. 244 CPP), respectivement le séquestre (art. 263 CPP), sont applicables⁷⁵.

[31] On relèvera que le CPP règle les modalités procédurales pénales, alors que la **LSCPT** en règle le déroulement technique (à l'exclusion du champ d'application⁷⁶), par exemple en définissant les **fournisseurs de services** de télécommunication (art. 2 et renvoi à l'art. 3 LTC) et leurs obligations (art. 26 ss LTC). Ceux-ci sont compris de manière large: il s'agit des fournisseurs d'accès Internet et de réseau mobile (par exemple Swisscom, Salt), de services de

---

⁶⁸ Le pendant pénal de la notion procédurale. Le débat dépasse la portée du présent article. Pour un aperçu, voir: COTTIER, p. 684 et JULEN BERTHOD, art. 263 CPP n° 20, réf. citées. La jurisprudence a confirmé l'analogie: [ATF 140 IV 181](#) c. 2.4, cité par BENHAMOU, p. 513, note 47.

⁶⁹ BENHAMOU, p. 8; BOMMER / GOLDSCHMID, art. 263 CPP n° 36; JULEN BERTHOD, art. 263 CPP n° 20, note 54.

⁷⁰ BENHAMOU, p. 9; COTTIER, p. 684.

⁷¹ Dans le même sens: COTTIER, p. 685, qui cite une position favorable également du CF et note la possibilité d'un blocage administratif, voir basé sur la clause générale de police (art. 36 al. 1 lit. 3 Cst), p. 686.

⁷² BENHAMOU / OETTLI, p. 217.

⁷³ Soit leur possession est interdite par l'art. 135 CP (HAGENSTEIN, art. 135 CP n° 110), soit il s'agit de matériel de propagande à détruire (BOMMER / GOLDSCHMID, art. 263 CPP n° 36; JULEN BERTHOD, art. 263 CPP n° 7 et 19). Voir également: [arrêt du TPF SK.2019.63](#) dispositif.

⁷⁴ Et soumis donc l'aval du TMC: JULEN BERTHOD, art. 263 CPP n° 21a, note 62; MÉTILLE, intro art. 269 à 281 CPP n° 8. Le secret couvre autant le contenu que les données accessoires.

⁷⁵ MÉTILLE, intro art. 269 à 281 CPP n° 44 à 46; DONATSCH et al., art. 246 CPP n° 8.

⁷⁶ [Arrêt du TPF SK.2013.39](#) c. 3.1.1; MÉTILLE, intro art. 269 à 281 CPP n° 48.

messagerie email (Gmail, Outlook), de chargement de données (Google docs) ou de communication entre usagers type *chats* (Facebook, Whatsapp, Skype), entre autres⁷⁷.

[32] À ce propos, on relèvera brièvement une **jurisprudence houleuse** par rapport aux services fournis par Facebook (réseau social) et Google (Gmail): le TF a jugé que ces services ne faisaient pas partie des télécommunications, puisqu'ils ne fournissent pas d'accès à Internet (alors qu'il en avait jugé autrement pour Facebook auparavant). Dès lors, le ministère public pouvait obtenir les données en question directement par un ordre de dépôt (art. 265 CPP) sans passer par une surveillance.⁷⁸ Ultérieurement, le TF a jugé que Facebook était un fournisseur dérivé de télécommunications, toujours sans que la surveillance ne s'y applique⁷⁹. Cette problématique n'a plus lieu d'être en ce qui concerne le statut de fournisseurs de télécommunication des réseaux sociaux, en vertu du nouvel art. 2 lit. c LSCPT; toutefois, la doctrine reste partagée sur la question de l'usage du dépôt (art. 265 CPP) en lieu et place de la surveillance (art. 269 CPP)⁸⁰.

[33] Selon nous, si c'est à juste titre que les réseaux sociaux sont considérés comme fournisseurs (dérivés) de télécommunications, et bien que le pragmatisme dicterait l'obligation de dépôt pour s'épargner les difficultés d'une entraide internationale, il semble néanmoins que l'obtention des messages envoyés via les réseaux sociaux relève bien d'une surveillance, et non d'un séquestre potentiel de données auprès des fournisseurs. La position du TF est dès lors critiquable.

[34] Pour en revenir à la surveillance offerte par les art. 269 ss CPP, celle-ci est soumise à des conditions strictes, que nous ne développerons pas ici⁸¹. Nous relevons simplement que la plupart des comportements incriminés par la **propagande terroriste** évoqués (*supra* I.B à D) tombent sous le coup de la disposition (art. 135, 226, 259, 260^{ter} et 261^{bis} CP, art. 74 al. 4 LRens). La surveillance au sens de l'art. 269 CPP est ordonnée par le ministère public puis autorisée par le TMC, elle est adressée au **Service SCPT**⁸² qui exploite un système informatique de traitement des données (art. 6 LSCPT), dont le but est de récolter les données pertinentes (comprenant les contenus mais également les métadonnées, art. 8 et 26 LSPCT), de les mettre à disposition des autorités pénales (art. 9 LSCPT), de les sécuriser et éventuellement de permettre leur analyse (art. 7 LSCPT). Les données sont obtenues auprès des fournisseurs de services numériques (y compris dérivés), qui ont l'obligation de les fournir si les conditions de la surveillance sont remplies (art. 26 ss LSCPT). Outre les données, certains renseignements

---

⁷⁷ *Ibid*, n° 26 à 34, 54. **Critique** la largeur du champ d'application: n° 31. Notons que les réseaux internes d'entreprises ne sont pas inclus: *ibid*, n° 58.

⁷⁸ [ATF 143 IV 21](#) c. 3.1 (Facebook), [arrêt du TF 1B 142/2016](#) c. 3.1 (Google), par opposition à l'[ATF 141 IV 108](#) (auparavant).

⁷⁹ [ATF 143 IV 270](#) c. 4.8 et 7.1.

⁸⁰ Indépendamment de l'emplacement en Suisse ou à l'étranger des données ou du siège du fournisseur. Semblent **contre**: BENHAMOU / OETTLI, p. 212; JULEN BERTHOD, art. 263 CPP n° 21a et note 62; MÉTILLE, intro art. 269 à 281 CPP n° 35. Semblent **pour**: THORMANN / BRECHBÜHL, art. 246 CPP n° 4; DONATSCH et al., art. 246 CPP n° 8a.

⁸¹ Voir: MÉTILLE, art. 269 CPP n° 12 à 32.

⁸² Art. 3 LSCPT; MÉTILLE, art. 269 CPP n° 3 et 9.

sont également obligatoires (comme les coordonnées de l'utilisateur, les adresses IP, ou « toute indication » au sens large, art. 21 et 22 LSCPT)⁸³.

[35] Si cette surveillance est restée sans succès ou n'a aucune chance d'aboutir, l'autorité peut également ordonner l'utilisation de **dispositifs techniques spéciaux** au sens de l'art. 269^{bis} CPP, comme un IMSI-Catcher. Il s'agit de simuler une antenne téléphonique, de sorte que les téléphones présents dans son champ s'identifieront auprès de cette base, permettant donc d'identifier un numéro SIM ou IMEI, de géolocaliser et d'écouter les conversations téléphoniques et ce, sans une quelconque collaboration du fournisseur⁸⁴.

[36] L'autorité peut également ordonner l'utilisation de **programmes informatiques spéciaux** introduits dans un système informatique, afin d'en intercepter puis d'en transférer les communications et données secondaires, au sens de l'article 269^{ter} CPP. Il s'agit essentiellement pour la police d'installer, à la manière d'un « cheval de Troie », un GovWare dans un ordinateur ou un *smartphone*, à l'insu de son propriétaire et en exploitant une faille, afin d'en prendre le contrôle et donc de surveiller son activité. Cela permettra de lire des conversations chiffrées de bout en bout⁸⁵: une perquisition « *en ligne* » des supports reste interdite⁸⁶.

[37] Enfin, dans le cas où les preuves numériques ne proviendraient pas d'un support détenu par l'auteur ou d'une surveillance des communications, mais seraient détenues par un tiers (comme Google ou Facebook, vu *supra*), l'**ordre de dépôt** de l'art. 265 CPP permet, sans mesure de contrainte⁸⁷, de demander au détenteur des données de fournir celles-ci. Relevons qu'il couvre tant les données stockées localement sur un support que les données stockées sur un serveur distant et inaccessible⁸⁸, avec toutefois la difficulté citée plus haut relativement aux serveurs situés à l'étranger.

C. Méthodes de recherche

[38] Le cadre juridique ayant été posé, les chapitres suivants traiteront uniquement de l'aspect technique de la récolte des preuves numériques. Tout d'abord, elles doivent être détectées et reliées à un auteur grâce à des éléments intrinsèques ou externes.

1. Détection

[39] Bien que, comme nous l'avons vu, il n'existe pas de surveillance générale d'Internet, il est possible, malgré l'absence d'ouverture d'une procédure pénale (ou plutôt avant celle-ci), de détecter⁸⁹ des preuves numériques liées au terrorisme par la recherche d'informations

⁸³ Relevons que le contenu des communications est régi par l'art. 270 CPP, alors que les renseignements liés à l'identification relèvent de l'art. 273 CPP: MÉTILLE, art. 270 CPP n° 5.

⁸⁴ Même contre un refus de collaborer. MÉTILLE, art. 269^{bis} CPP n° 4 et 5.

⁸⁵ THORMANN / BRECHBÜHL, art. 246 CPP n° 4; MÉTILLE, art. 269^{ter} CPP n° 1, 5, 8 et 11; PAJAROLA, p. 250.

⁸⁶ HOHL-CHIRAZI, art. 246 CPP n° 20. Ce terme est néanmoins utilisé, par abus de langage: PLATZ, pt I.1.

⁸⁷ [ATF 143 IV 21](#) c. 3.1; BENHAMOU / OETTLI, p. 211; MÉTILLE, intro art. 269 à 281 CPP n° 5.

⁸⁸ BENHAMOU / OETTLI, p. 212.

⁸⁹ Au sens forensique, il s'agit simplement d'identifier les traces pertinentes: JAQUET-CHIFFELLE, p. 196. Les plateformes de réseaux sociaux (Youtube, Facebook, Google+) disposent d'algorithmes de détection de contenus, cependant insuffisants: CEP, [Extremist Content](#), p. 2.

publiquement accessibles sur Internet, ce que l'on nomme **OSINF**⁹⁰. Ces informations sont une source importante pour les enquêtes pénales, du fait que l'Internet est utilisé partout et par chacun (surtout les réseaux sociaux)⁹¹. Beaucoup d'informations même supprimées ou rendues privées ultérieurement (par exemple une vidéo de propagande terroriste postée sur un forum puis effacée ensuite ou rendue privée) sont susceptibles d'être néanmoins retrouvées, puisque « *Internet a de la mémoire* »⁹²: on pensera à l'outil *Wayback Machine* de la fondation Archive.org, qui parcourt l'entier du web afin de le « *photographier* » et d'en garder une archive, consultable publiquement; il faut également partir du principe qu'un contenu publié même brièvement sur Internet a pu être sauvegardé par un tiers, et donc potentiellement propagé.

[40] La recherche sur des pages Internet et les réseaux sociaux implique une quantité phénoménale de données (typiquement relatives au contenu). Des outils de **recherche avancée** permettent d'affiner les résultats, par exemple en spécifiant des localisations ou des dates, ou en excluant des formats (images, vidéos)⁹³. Dans le cas d'une veille ciblée sur un site ou un thème particulier (terrorisme), on songera à la possibilité de « *scanner* » les publications par un terme précis (« #terro », « #ISIS »), ou d'utiliser une IA pour ce faire. Enfin, des outils comme THB Liberi permettent de scanner à intervalles réguliers un site ou forum donné et d'en détecter les changements. Puisque chaque site ou forum peut avoir une structure particulière, il faudra parfois que la police crée un programme spécifique à cette fin.

[41] Cette recherche OSINF ne nécessite pas de mandats particuliers et peut se faire librement par la police, dans les limites suivantes: une interaction avec la cible ou sa publication (comme une demande d'ami ou un « *like* ») est proscrite, car celle-ci ressort des recherches secrètes (avant la procédure: art. 298a ss CPP; après: art. 70 LPol-NE) et est réservée à des agents de police judiciaire spécialisés; dans le cadre d'enquêtes sensibles (typiquement le terrorisme), il existe des risques pour l'intégrité de l'agent ou de l'institution, ou de compromission de l'enquête; enfin, la recherche se fera exclusivement avec les infrastructures policières et des comptes d'utilisateurs créés à cette fin, par mesure de sécurité et pour éviter un traçage ou une erreur. La recherche OSINF présente des **désavantages** au niveau de la fiabilité (que nous développerons plus bas), et de l'efficacité: vu la masse de données présente sur le web, il sera inévitable qu'un enquêteur passe à côté d'informations pertinentes par erreur, par manque d'expertise ou à cause de biais cognitifs influençant ses recherches⁹⁴. L'utilisation d'une IA permettrait de combler ces lacunes, mais elle souffre à son tour de ses propres limites, notamment de devoir être « *entraînée* » correctement et avec une base de données suffisante.

[42] Puis dans le cadre d'une procédure pénale, nous avons esquissé la possibilité d'utiliser un GovWare, soit un programme « *infiltrant* » le support d'une cible (ordinateur, *smartphone*) afin de détecter des preuves numériques. Le contexte policier parle de **Remote forensic software**. De manière technique, ses possibilités sont puissantes: il permet de consigner les frappes sur le clavier de l'utilisateur (et donc de découvrir ses mots de passe par exemple), de scanner de manière ciblée le système afin d'en trouver les données incriminées, de lire des conversations cryptées, et d'enregistrer via le microphone ou la caméra les actions de l'auteur⁹⁵. Son

⁹⁰ Circ. 2.111 de la PONE: Recherches sur Internet – Open Source Information (OSINF).

⁹¹ Guide, p. 160 et 161.

⁹² JACQUEMIN, p. 344 à 245.

⁹³ Guide, p. 161. Dans cette phase, on « ratissera large »: FURNER, p. 210.

⁹⁴ Europol, *Deepfakes*, p. 16; POLLITT et al., p. 3.

⁹⁵ PLATZ, pt II.1.

installation, nécessairement à l'insu de ce dernier, peut se faire par ouverture d'un lien envoyé par e-mail à la cible, ou par l'exploitation de failles de sécurité par une attaque en réseau. Puisque ces méthodes présupposent une imprudence de la cible ou une faiblesse du système d'exploitation (sans parler des nombreux systèmes différents), en plus de nécessiter des connaissances poussées du spécialiste policier, le *remote forensic software* est extrêmement difficile à installer et ne s'utilise que rarement en pratique⁹⁶.

2. Identification de l'auteur

[43] Au sens forensique, de manière large et incluant les domaines matériel et numérique, l'**identification** se définit comme un « *processus décisionnel tentant d'établir, avec suffisamment de confiance, qu'une information identitaire est liée à une entité spécifique dans un contexte donné à un certain moment* »⁹⁷. La décision se base sur au moins l'un des quatre éléments suivants: l'entité (une personne ou un groupement), l'information identitaire (la connexion à un compte d'utilisateur spécifique, une vidéo postée), le contexte (un forum de discussion sur le terrorisme) et le moment (une date ou un intervalle de temps)⁹⁸. Un seul élément peut suffire à fonder la confiance, mais bien sûr on cherchera à la renforcer par plusieurs d'entre eux.

[44] À cette fin et dans le domaine numérique, les **métadonnées** (les données relatives à l'abonné et au trafic) sont d'une importance capitale pour le travail policier. **En ligne**, les images (sous format EXCIF) ou vidéos postées sur des forums ou des réseaux sociaux peuvent contenir des informations telles que les coordonnées du lieu où la photo/vidéo a été prise, la date et l'heure, le type d'appareil voire même son utilisateur⁹⁹. Dans de rares cas, le numéro de série de l'appareil pourrait permettre de remonter, via une demande au fabricant, au magasin commercialisant l'appareil et à l'acheteur. Les emails contiennent des informations sur la date et l'heure, et surtout les adresses IP des expéditeurs, qui sont ainsi localisables ou identifiables simplement grâce à des sites comme ip-adress.com ou fr.geoipview.com¹⁰⁰. Enfin, les discussions sur réseaux sociaux permettent, via une demande au fournisseur, d'obtenir des informations sur l'utilisateur. Dans le contexte du terrorisme, les données principales seront les fichiers publiés (images, vidéos), les adresses IP des utilisateurs (sur forums, sites web) et les historiques de conversations sur réseaux sociaux, comme Telegram.

[45] Toutefois, cette méthode trouve sa **limite** en présence d'un auteur prudent ou méticuleux, qui pourra aisément rendre impossible sa localisation via son adresse IP en utilisant un *virtual private network* comme NordVPN. De même, le cryptage (aussi proposé par NordVPN) croissant des interactions sur le web rend difficile voire impossible l'identification de l'utilisateur « *depuis l'extérieur* » (i. e. en surveillant son trafic) sans une perquisition du support ou la prise de contrôle par un *remote forensic software*¹⁰¹. Enfin, et contrairement au Guide, les spécialistes de la PONE mettent en doute la « *richesse* » en métadonnées des fichiers postés en ligne: en effet, certains sites web ou réseaux sociaux (n. Instagram) modifient les fichiers *uploadés* par l'utilisateur afin

⁹⁶ *Ibidem*.

⁹⁷ POLLITT et al., p. 7, notre traduction.

⁹⁸ *Ibid*, nos exemples.

⁹⁹ Guide, p. 161 à 162. Des informations issues du contenu lui-même permettent parfois d'identifier l'auteur d'une photographie, comme un flash qui refléterait son visage ou la reconnaissance du lieu de la photographie.

¹⁰⁰ *Ibid*, p. 162.

¹⁰¹ PLATZ, pt I.1; PAJAROLA, p. 251.

d'en réduire sa taille, supprimant de ce fait tout ou partie des métadonnées. Ainsi, ces fichiers serviront principalement à l'identification liée au contenu, et non à celle liée aux métadonnées.

[46] L'identification de l'auteur via des OSINF présente également des **problèmes de fiabilité**: des sites non officiels permettent à n'importe quel tiers de lier des métadonnées à un contenu, palliant certes ainsi leur suppression par des réseaux sociaux, mais rendant celles-ci non suffisamment fiables pour une utilisation judiciaire.

[47] Si un **support numérique** est disponible (par saisie), l'identification de l'auteur en sera grandement simplifiée. Outre l'information identitaire (si un fichier se trouve sur l'ordinateur d'un individu, cela suffira dans la plupart des cas à l'incriminer), les *smartphones* et les ordinateurs regorgent de métadonnées liées au contexte et au moment¹⁰². D'une part, toute page Internet consultée est en réalité téléchargée sur le support (l'expression « *se rendre sur* » un site Internet est un abus de langage; en réalité c'est la page Internet qui se rend sur la machine de l'internaute¹⁰³), et donc ses métadonnées (dates de connexion, utilisateur, fichiers consultés) sont consultables au moins dans la mémoire cache si la consultation est récente. D'autre part et en présence d'un *smartphone*, les données téléphoniques révèlent des informations quant aux messages émis et reçus, l'identité de l'utilisateur, l'heure et la durée des appels, et la géolocalisation¹⁰⁴. De même, la difficulté des contenus de conversations cryptées est levée, puisque le cryptage « *de bout en bout* » concerne principalement le cheminement entre supports: à réception sur celui-ci, la conversation est claire et lisible. Enfin, dans une certaine mesure qui dépend de beaucoup de paramètres (système d'exploitation, type de disque dur, temps écoulé), la suppression de fichiers (sur un ordinateur par exemple) ne les efface pas entièrement du support, de sorte que des bribes de fichiers et donc des métadonnées restent accessibles¹⁰⁵.

[48] On terminera cette section en relevant qu'au sujet de l'identification de l'auteur liée aux métadonnées mais aussi au **contenu**, la plupart des polices cantonales font face à la difficulté d'une absence de base légale permettant un échange automatique d'informations entre cantons¹⁰⁶. Les Romands ont développé des outils d'échanges d'informations pour les infractions cyber, notamment la *Plateforme d'Informations de la Criminalité Sérielle En Ligne* (PICSEL). Le but est ainsi de faciliter l'identification d'un auteur grâce aux informations déjà obtenues par d'autres polices (cantonales¹⁰⁷), mais aussi d'informer sur des nouvelles manières de procéder des criminels (les *modus operandi*) et donc de renforcer la prévention¹⁰⁸.

D. Méthodes de saisie

[49] Une fois l'auteur identifié, ou en cas de soupçons à son égard justifiant une perquisition de son matériel, les autorités chercheront à saisir ses supports physiques ou à sauvegarder d'une

---

¹⁰² Guide, p. 162.

¹⁰³ TIRELLI, p. 25.

¹⁰⁴ Guide, p. 163.

¹⁰⁵ FURNER, p. 211.

¹⁰⁶ Rapport du CF, *Cybercriminalité*, p. 19. Neuchâtel dispose de telles bases légales: art. 38 LPol-NE, ainsi que le [Concordat réglant la coopération en matière de police en Suisse romande](#) (RS-NE 561.3), particulièrement à son art. 5 lit. b concernant le terrorisme.

¹⁰⁷ Le volet de coopération internationale dépasse largement la portée du présent article. Pour un aperçu, n. concernant Interpol et Europol, voir CARTIER, p. 66 ss.

¹⁰⁸ CARTIER, p. 62, 63. Concerne surtout la cybercriminalité au sens strict.

autre manière les données en ligne (*cloud*, etc.). La saisie des données répond à plusieurs principes.

- D'une part, son but est la **préservation** des preuves en évitant toute altération de celles-ci pour assurer la suite des activités forensiques (authentification, comparaison, etc.) et légales (mise en accusation, jugement)¹⁰⁹. Outre les changements externes (manipulation de tiers, accès à distance), certaines données subissent des modifications à cause de leur « *dynamique interne* », qu'il s'agira de minimiser (par exemple, refroidir la mémoire d'un ordinateur qui « *tourne* » à plein régime, ou figer par capture d'écran un historique de localisations avant leur effacement)¹¹⁰.
- D'autre part et vu la complexité grandissante du numérique, la présence d'un **expert** sera probablement nécessaire, non seulement pour l'exploitation ultérieure des données mais surtout au stade de la saisie¹¹¹. On pensera notamment au cas où l'auteur/la cible est versé dans l'informatique. Des auteurs ont d'ailleurs mis le doigt sur les carences en matière de savoir ou de formation des enquêteurs des autorités pénales, ainsi que sur la difficulté de maintenir une expertise dans un domaine qui évolue de manière très rapide, surtout en compétition avec le secteur privé¹¹². Dès lors et dans le doute, un enquêteur (ici, de la PONE) fera toujours appel aux experts de l'IN.

[50] L'expert sera également nécessaire au vu de la **masse de données** à saisir ou mettre en sûreté: au contraire des perquisitions matérielles normales, même pour des enquêtes de grande ampleur (on pensera par exemple aux milliers de plans de cannabis dans un cas de trafic de stupéfiants, ou aux pièces comptables d'une grande société réparties dans d'innombrables classeurs fédéraux dans un cas de criminalité économique), le numérique implique une quantité colossale de données virtuelles. Ce qui pose des difficultés pour leur saisie (temps, personnel à disposition), leur conservation (infrastructures) et leur tri¹¹³: ainsi, on procèdera à la saisie de tous les supports pertinents, mais on limitera dans un premier temps l'analyse aux appareils les plus susceptibles de renfermer les preuves (tablettes ou *smartphone* par exemple, en laissant de côté les clefs USB et les GPS)¹¹⁴.

[51] Enfin, on n'insistera jamais assez sur l'importance du respect des mesures décrites ci-après, à cause de la **fragilité et de la volatilité** extrêmes des preuves numériques par leur nature¹¹⁵, ce qui dictera également l'urgence et les mesures à prendre pour leur saisie. Les risques incluent la modification à distance par un tiers (consciente ou non), l'écrasement des données par le support lui-même, l'extinction de l'appareil faute de charge et donc la difficulté d'accéder à son contenu, ou même la modification par une utilisation normale du support (réception de messages, déplacement de géolocalisation).

¹⁰⁹ Guide, p. 164; JAQUET-CHIFFELLE, p. 197; PLATZ, pt II. 2; POLLITT et al., p. 12.

¹¹⁰ JAQUET-CHIFFELLE, p. 197.

¹¹¹ FURNER, p. 210; Guide, p. 165.

¹¹² CARTIER, p. 75; Europol, *Deepfakes*, p. 15; FURNER, p. 211.

¹¹³ BENHAMOU/OETTLI, p. 210; FURNER, p. 211.

¹¹⁴ FURNER, p. 210.

¹¹⁵ FURNER, p. 210; DONATSCH et al., art. 246 CPP n° 8a; PLATZ, pt II.2; Circ. 2.107 A05 de la PONE: Saisies et perquisitions en lien avec du matériel informatique.

1. Protocoles

[52] La priorité de prise en charge des **supports numériques**, lors d'une perquisition par exemple, sera principalement déterminée par l'urgence et par le risque de détérioration des données. Ainsi, un appareil allumé et déverrouillé sera prioritaire par rapport à un appareil verrouillé ou éteint (dans ce cas, une modification est en principe impossible). La première chose à faire est de mettre l'appareil hors réseau, par exemple en activant le « *mode avion* » ou en désactivant le wifi et/ou le *bluetooth*, ou en le plaçant dans un « *sachet de faraday* »¹¹⁶. Pour un ordinateur, on débranchera le câble réseau et on désactivera le wifi et/ou *bluetooth*.

[53] Si un support est déverrouillé, on cherchera à le maintenir en cet état, par exemple en effectuant des mouvements de souris (ordinateur ou *smartphone*) ou en prolongeant par le menu le mode veille ou le verrouillage¹¹⁷: un support verrouillé sera plus difficile à explorer en l'absence du mot de passe de l'utilisateur (voir plus bas). De surcroît et pour la même raison, on n'éteindra pas un appareil allumé. Enfin, ce sera toujours la police (enquêteur ou expert IN) et non l'auteur qui manipulera le support.

[54] En présence d'un support éteint, il faudra le laisser dans cet état et ne pas essayer de l'allumer, même en connaissance du mot de passe/code de déverrouillage¹¹⁸: le démarrage entraîne inmanquablement une modification des données, et en principe un appareil éteint est sécurisé. On pourra cependant retirer la carte SIM, afin d'éviter une mise en réseau (automatique) par certaines applications.

[55] Il est intéressant de relever les **difficultés** rencontrées, même par les professionnels, lors de la perquisition de supports verrouillés car éteints, protégés par un mot de passe ou un code de déverrouillage. Le fait de pouvoir « *craquer* » (*i. e.* accéder à son contenu) n'importe quel support relève plutôt de la fiction que de la réalité: les limites temporelles liées à l'essai systématique de combinaisons jusqu'à trouver la bonne (technique nommée *brut force*) sont insurmontables, surtout en présence de clefs de cryptage ou de mots de passe générés par informatique et donc d'une longueur conséquente. Souvent, des imprudences de l'auteur permettent de contourner le problème (mot de passe écrit sur un *post-it*, code reprenant une date de naissance, phrase simpliste et en rapport avec le sujet/site, etc.). Mais en l'absence d'imprudence, force est de constater qu'il est parfois **impossible de craquer** un support numérique. L'obtention du mot de passe de l'auteur est capitale.

[56] Concernant les **données en ligne** (*clouds*, serveurs des réseaux sociaux), leur saisie est confrontée aux mêmes difficultés: il y sera en principe toujours accédé depuis le support de l'auteur, et son mot de passe est dès lors capital au risque de devoir passer par l'entraide internationale, d'une grande lenteur. Enfin, la saisie des données en ligne se résume à en capturer le contenu (capture d'écran, code source de la page web) et encore, seulement les données transmises jusqu'à la dernière connexion de l'utilisateur, seul le fournisseur étant en mesure de fournir les métadonnées. La saisie de données en ligne requiert, par mesure de sécurité, l'utilisation d'une connexion Internet dissociée du réseau de l'entreprise/de l'administration.

---

¹¹⁶ Poche bloquant les ondes électromagnétiques. Ce procédé déchargera la batterie.

¹¹⁷ Toutefois sans enlever le code de verrouillage, cela supprimerait les données utilisateur.

¹¹⁸ PLATZ, pt II. 2.

[57] Enfin, une fois le support obtenu, la procédure exige d'en copier le contenu de la manière la plus complète possible, soit d'en faire une **copie forensique** comprenant les métadonnées en vue de son authentification¹¹⁹. De manière technique, le support (ordinateur, disque dur ou clef USB) est connecté à l'ordinateur de l'IN, qui dispose d'un *bloqueur en écriture*¹²⁰, garantissant que les données ne circulent que d'une manière unilatérale et ne pourront donc être que lues, sans modification (par une interaction). Ce procédé est chronophage, et ne fonctionne pas pour les *smartphones*, qui disposent d'un système de cryptage empêchant l'extraction de données. De même, certains disques durs sont automatiquement chiffrés lorsqu'ils sont « *désolidarisés* » de leur support, empêchant leur lecture. La saisie des preuves numériques est ainsi close: l'étape suivante sera de les authentifier puis de les conserver.

2. Dangers

[58] La saisie des preuves numériques n'est pas exempte de certains dangers. Tout d'abord, les infrastructures policières ne sont pas à l'abri d'une **attaque cyber** de la part de pirates ou de groupements spécialisés (on pourrait penser à une « *division cyber* » d'un groupe terroriste), ce qui implique de devoir sécuriser les données numériques sur des serveurs distincts d'autres domaines de la police. Il n'y a en effet pas de locaux de stockages des supports saisis, toutes les données étant sauvegardées en ligne. Cette manière de faire demande également des réflexions pour sécuriser l'espace physique des serveurs utilisés, soit la « *salle des serveurs* » de l'infrastructure étatique. À Neuchâtel et en général, il s'agit de locaux enterrés et bétonnés de type abris antiatomiques, et placés sous alarme.

[59] Un deuxième danger réside dans de potentiels **virus** incorporés ou liés à des données numériques saisies chez un auteur. En pratique, les spécialistes se fient généralement à leur instinct: si l'auteur ne semble pas versé dans l'informatique (et en l'absence de préparation possible si la perquisition s'est faite par surprise), les supports seront ouverts via l'ordinateur normal de l'expert IN, protégé le cas échéant par un antivirus. En cas de doute ou de danger concret, le support sera ouvert ou lu par un ordinateur *froid* soit hors réseau, ou via une *sandbox* (programme créant un espace hermétique et non communiquant avec le reste du système). On relèvera enfin que le format d'un virus est en principe lié à un système d'exploitation: l'usage d'un tel système différent de celui du support pourra réduire les risques d'infection.

[60] Enfin, on présentera un danger d'aspect humain dans la saisie des preuves numériques, surtout dans le cadre du terrorisme (et également en pédopornographie): les preuves liées prenant souvent la forme d'images choquantes et sanglantes, leur exposition aux enquêteurs qui en analysent une grande quantité peut **affecter leur psychisme** et induire une forme de stress, voir des traumatismes. Pour pallier cela, il est possible de flouter les images dans leur mode lecture (donc sans altérer la qualité de l'image d'origine) ou d'en réduire la taille à une miniature, afin d'en limiter l'exposition néfaste pour l'enquêteur.

---

¹¹⁹ BENHAMOU / OETTLI, p. 217.

¹²⁰ Ou *write blocker*, JAQUET-CHIFFELLE, p. 200.

II. Les problématiques liées à l'administration des preuves

[61] Une fois saisies, les preuves numériques doivent être analysées, triées et sauvegardées par la police afin d'être transmises au ministère public ou aux tribunaux. Nous nous concentrerons ici sur les étapes forensiques de l'authentification, de la conservation et de la sauvegarde¹²¹.

A. Authentification

[62] **L'authentification** est, au sens forensique large, un « *processus décisionnel tentant d'établir la vérité d'une proposition avec suffisamment de confiance* »¹²². Il s'agira en somme pour la police ou le ministère public de montrer que l'auteur présumé et identifié est bien coupable de(s) l'infraction(s) retenue(s), sur la base des preuves administrées. En termes légaux, la « *confiance suffisante* » dépend des circonstances, des procédures et des questions de droit en cause: on parlera ainsi parfois de « *certitude* », de « *vraisemblance* » ou de « *soupçon* ». En droit pénal, le principe de la présomption d'innocence – *in dubio pro reo* – de l'art. 10 al. 3 CPP exige l'absence de « *doutes insurmontables* »: nous relèverons ici que la notion de confiance, au sens forensique, n'exige **pas de certitude** ou de confiance absolue, qui n'est ni réaliste, ni réalisable. Les preuves (numériques) doivent permettre de manière « *suffisamment sûre* » d'incriminer l'auteur¹²³. La police, ici l'IN, évaluent celles-ci par un degré de probabilité (appelé **force indiciaire**) basé sur un ressenti intuitif, non exprimé en valeurs numériques¹²⁴.

[63] L'authentification d'une donnée ou d'un fichier peut reposer sur une **comparaison** avec d'autres éléments, numériques ou analogiques, comme la reconnaissance vocale (issue d'un enregistrement et comparée à la voix), l'identification faciale (extraite d'une vidéo ou d'une image et comparée à une base de données ou à d'autres images préalablement authentifiées) ou l'analyse de vidéos ou d'images quant à la réalité de ce qu'elles représentent¹²⁵. Des outils similaires ont également été développés à l'usage des réseaux sociaux, comme le programme eGLYPH permettant de détecter du contenu terroriste, d'en extraire une signature électronique qui est comparée à d'autres contenus *online*¹²⁶. Une grande partie, voire la quasi-totalité, de l'authentification passe par l'analyse des **métadonnées** d'un fichier. Ainsi et en pratique, l'adresse IP d'un email ou d'un profil d'utilisateur sur un forum ou un réseau social, reliée par une identification de l'utilisateur donnée par le fournisseur, suffira à authentifier qu'il est bien l'auteur du comportement incriminé (propagande terroriste par exemple). La perquisition de ses supports informatiques rend cette tâche plus facile, car l'entier des métadonnées est à la disposition des enquêteurs¹²⁷.

[64] Les données recueillies se présentent sous un format binaire, il est donc nécessaire de disposer d'un programme de « *lecture* » dont la tâche sera, outre d'inventorier toutes les

¹²¹ Pour un aperçu général du processus forensique entier, voir POLLITT et al., p. 10 ss.

¹²² POLLITT et al., p. 7, notre traduction.

¹²³ JAQUET-CHIFFELLE, p. 204. La dernière personne devant s'en convaincre est le juge: POLLITT et al., p. 9.

¹²⁴ Dans certains domaines des sciences forensiques, en présence d'éléments comme l'ADN pouvant faire l'objet d'une mesure probabiliste, on parlera parfois d'une probabilité « 2000 fois supérieure à ... ».

¹²⁵ POLLITT et al., p. 2.

¹²⁶ CEP, *Extremist Content*, p. 2.

¹²⁷ Sans compter que dans la plupart des cas, la seule présence d'un fichier sur le disque dur ou dans l'ordinateur du prévenu suffira à l'incriminer, par exemple selon l'art. 135 CP.

données, de les présenter sous forme lisible. L'IN et les enquêteurs de la PONE utilisent le *software Cellebrite*¹²⁸, qui permet de présenter chaque donnée sous sa forme lisible: une adresse IP (suite de caractères), une géolocalisation (idem, ou incorporée directement sur une carte), une image, une vidéo ou un texte. Il offre également des outils de tri des données, en excluant par exemple les fichiers en deçà d'une certaine taille, et en permettant de « *taguer* » les éléments d'une certaine couleur afin de les différencier (selon leur importance, l'infraction en cause, etc.). Ce programme se veut simple d'utilisation et accessible même à un enquêteur non spécialiste: toutefois, l'IN effectue parfois ce travail en amont. Enfin, on relèvera que pour chaque analyse d'un élément de preuve électronique, les actions effectuées (extraction, sauvegarde, tri et présentation lisible) devront impérativement être consignées de manière à ce qu'un tiers puisse, le cas échéant, les refaire¹²⁹.

[65] À cause de (ou plutôt grâce à ?) la nature numérique des données, la suppression d'un fichier (par l'utilisateur ou indépendamment de sa volonté) laisse parfois subsister des bribes de celui-ci. Si cela permet d'en récupérer des éléments pertinents, une conséquence négative sera également qu'il sera moins lisible, ou détérioré. De même, des fichiers intacts (une image, une vidéo) peuvent présenter des défauts de visibilité résultant de leur création (prise de vue rapide, de loin, etc.). Ainsi, l'authentification d'une donnée passe parfois par la nécessité d'« **améliorer** » les preuves¹³⁰: par exemple, pour une photo floue ou prise dans l'obscurité, des *softwares* permettent via des algorithmes d'améliorer les contrastes ou de préciser des contours. Ce procédé ne crée pas d'information à proprement parler, mais l'améliore. Dans d'autres cas, en présence de fichiers détériorés, il s'agira cette fois-ci de créer de l'information afin de compléter ceux-ci pour en rendre la lecture possible, par exemple en ajoutant des contours corporels autour d'un visage sur une vidéo floue¹³¹. À nouveau, on rappellera l'importance de protocoler toute modification du fichier original.

[66] Nous terminerons cette section en soulevant brièvement une problématique récente en matière d'authentification liée à l'IA, à savoir les **deepfakes**. Certains auteurs les érigent en effet en l'une des menaces principales actuelles de notre société¹³², et Europol les évoque en tant que contenu favorisant les groupes extrémistes en tant que propagande¹³³. Nous renvoyons le lecteur à la littérature en ce qui concerne leur définition et leur fonctionnement¹³⁴. On relèvera en revanche que grâce à leur sophistication en matière de manipulation de contenu, les **deepfakes** posent des problèmes aux autorités pénales, notamment pour l'identification de l'auteur ou des faits pertinents, et parce qu'ils ébranlent la confiance en des moyens de preuve généralement considérés comme fiables et authentiques comme les images ou vidéos représentant des faits¹³⁵.

---

¹²⁸ Cellebrite (<https://cellebrite.com/en/cellebrite-software>).

¹²⁹ Guide, p. 165; JAQUET-CHIFFELLE, p. 198.

¹³⁰ POLLITT et al., p. 12.

¹³¹ Exemples de *softwares*: Amped FIVE (<https://ampedsoftware.com/five>), Topaz IA (<https://topazlabs.com>).

¹³² JACQUEMIN, p. 315.

¹³³ Europol, *Deepfakes*, p. 10. Dans le même sens et pour la désinformation, JACQUEMIN, p. 323.

¹³⁴ Voir: Europol, *Deepfakes*, p. 7 ss et JACQUEMIN concernant la définition (p. 316), le *machine* et *deeplearning* (p. 317 à 319) et les formes (p. 319 à 320).

¹³⁵ Europol, *Deepfakes*, p. 14 ss, également pour les défis futurs des forces de police.

[67] Au stade actuel, la plupart des contenus *deepfakes* créés ou modifiés par IA sont reconnaissables en tant que tels, grâce à des détails comme l'absence de clignements d'œil ou des contours flous ou non naturels des cheveux et des membres corporels¹³⁶. Au niveau des métadonnées, un contenu *deepfake* n'est pas identifiable comme tel, il ne possède pas de propriété intrinsèque démontrant l'intervention de l'IA. Le meilleur outil pour authentifier ou au contraire pour exclure un élément de preuve numérique reste l'œil affûté des spécialistes; toutefois et au vu de l'évolution rapide dans le domaine, celui-ci, même assisté d'une IA, ne suffira probablement plus pour détecter un *deepfake*¹³⁷.

B. Chaîne de conservation et sauvegarde à des fins judiciaires

[68] Pour garantir l'authenticité démontrée des preuves, il est capital que celles-ci soient conservées, ce qui signifie principalement d'en **éviter toute modification**¹³⁸. Ainsi, l'analyse par la police devra être non destructive pour préserver la chaîne d'intégrité: on procédera par exemple à une photographie ou à un enregistrement au préalable (pour des données en ligne en l'absence de métadonnées: des captures d'écran et de code source de la page Internet), à une description des buts et des méthodes de l'analyse, puis à la copie¹³⁹. Une copie est dite « parfaite » si le support n'a pas été altéré, et « pure » si l'information dans la copie est strictement identique à celle sur le support¹⁴⁰.

[69] En pratique, cette étape se fait déjà lors de la saisie des données: une fois celles-ci extraites (d'un support), avant ou après leur analyse, celles-ci sont stockées obligatoirement en réseau, pour des raisons de sécurité et de risque de perte des données. La police ne transmet en effet pas de supports *froids* et non-analysés aux tribunaux, mais des données lisibles. Puisqu'une numérisation est obligatoire, il s'agit alors, pour la conservation des données, de les accompagner d'un **certificat d'authenticité** qui enregistrera tout changement ou accès ultérieur à celles-ci: un journal retracera l'historique de chaque accès et de chaque personne en ayant eu l'accès¹⁴¹. Le but de toute preuve forensique est d'être compréhensible, démontrable et vérifiable¹⁴².

[70] Afin de prévenir les modifications intentionnelles des données (en vue de les fausser pour disculper l'auteur, ou au contraire afin de l'incriminer davantage¹⁴³), il est possible d'incorporer un **système d'horodatage**: techniquement, il s'agit de lier le certificat d'authenticité à un registre (type *blockchain*) où chaque action ou accès à la donnée est enregistré temporellement, de sorte que l'état d'une donnée est figé à un instant précis. Des accès ultérieurs s'ajoutent aux éléments précédents, mais ne peuvent modifier ceux-ci¹⁴⁴.

---

¹³⁶ *Ibid*, p. 16 et 17.

¹³⁷ JACQUEMIN, p. 319 et 324.

¹³⁸ FURNER, p. 210; PLATZ, pt II.2.

¹³⁹ FURNER, p. 211; JAQUET-CHIFFELLE, p. 198.

¹⁴⁰ JAQUET-CHIFFELLE, p. 200.

¹⁴¹ FURNER, p. 210; JAQUET-CHIFFELLE, p. 201.

¹⁴² FURNER, p. 210.

¹⁴³ Dans les deux cas, la conséquence pourrait être l'inadmissibilité de la preuve, voire une sanction pénale: Guide, p. 164

¹⁴⁴ Voir: JAQUET-CHIFFELLE, p. 202 à 203 pour les détails techniques.

[71] La transmission des preuves numériques aux tribunaux suppose, pour les données prélevées sur des supports, de rendre celles-ci lisibles. Dans la pratique, les copies (forensiques) des données ne sont pas transmises telles quelles, la plupart des autorités judiciaires ne disposant pas d'une infrastructure suffisante pour leur stockage ni des compétences techniques pour leur analyse. Bien plutôt, les analyses seront présentées de manière lisible dans un rapport technique au juge, avec référence aux données qui, elles, restent sur les serveurs de la police. Dans le cas des preuves en ligne liées au contenu et donc exemptes de métadonnées, elles pourront être transmises simplement sur un CD-R au tribunal.

Conclusion

[72] La propagande terroriste, majoritairement sous la forme de publications, de partage de contenu et de diffusion de liens en ligne, a désormais une réalité concrète et croissante sur les réseaux sociaux, et de manière plus générale sur l'Internet au travers de forums, de *chats* et d'autres blogs. En l'état actuel, le droit pénal suisse est suffisant pour punir les différents comportements constitutifs de propagande terroriste. Toutefois, les difficultés se présentent au niveau procédural, surtout dans la détection, la recherche ou la saisie des preuves.

[73] De manière préventive, aucune loi n'oblige les fournisseurs de services en ligne, au sens large, à veiller au contenu diffusé sur leurs serveurs, ni à fournir leurs données autrement que de manière volontaire. De même, il n'existe pas de surveillance générale d'Internet par les services étatiques. La LRens fédérale permet, dans certaines conditions, d'effectuer des recherches secrètes, mais celles-ci, incluant des mesures de contrainte, sont assorties de la nécessité d'obtenir l'autorisation préalable des autorités. Le seul moyen de s'en affranchir étant la recherche d'OSINF, qui est également prévue par le droit cantonal mais qui suppose tout de même une approche ciblée (sur un contenu, un auteur, un site).

[74] Durant la procédure pénale, donc en présence de soupçons concrets, les autorités pénales peuvent procéder à des perquisitions, à des saisies et à des séquestres, voire à la surveillance des télécommunications, éventuellement avec des dispositifs techniques spéciaux comme l'IMSI-Catcher ou le GovWare. L'accès aux données en ligne (souvent stockées sur des serveurs situés à l'étranger) nécessite l'entraide internationale, chronophage et donc peu efficace en regard de la rapidité de circulation des données dans le monde numérique.

[75] Les difficultés pratique et technique de ces moyens d'obtention des preuves, sur des supports numériques ou en ligne, sont nombreuses. Elles englobent l'identification de l'auteur, notamment grâce aux métadonnées; la saisie des données, rendue difficile par leur volatilité, leur masse et souvent par leur chiffrement; leur conservation et la nécessité d'en éviter toute altération, donc par le biais de procédés qui en garantissent l'intégrité; leur présentation sous forme lisible et exploitable, y compris en présence de « *fragments* » de fichiers; l'authentification des contenus, qui subit la prolifération des *deepfakes* peu détectables et qui nécessite souvent d'améliorer certaines preuves; enfin, la transmission aux ministères publics et aux tribunaux, afin que la condamnation de l'auteur – le stade ultime de la chaîne pénale – soit rendue possible.

[76] Au vu de l'évolution permanente et exponentielle du monde digital, ces difficultés et défis iront assurément croissant durant les prochaines années, et exigeront des adaptations rapides de l'État (en termes de législation, de personnel et d'entraide notamment) s'il entend garder un certain contrôle sur cet univers virtuel et les infractions qu'il rend possible, inévitables contreparties de la liberté d'opinion au sens large.

Bibliographie

Doctrine

- AJIL Ahmed / LUBISHTANI Kastriot, *Le terrorisme djihadiste devant le Tribunal pénal fédéral, Analyse des procédures pénales de 2004 à 2020*, in: Jusletter Weblaw, 31 mai 2021.
- BENHAMOU Yaniv, *Blocage de sites web en droit suisse: des injonctions civiles et administratives de blocage au séquestre pénal*, in: Droit d'auteur 4.0., 2018, p. 1-27.
- BENHAMOU Yaniv / OETTLI Jean-René, *Traitement des données par les autorités pénales: de l'accès aux données à la procédure de tri*, RPS 139/2021, 209 – 233.
- BOMMER Felix / GOLDSCHMID Peter, Art. 263 CPP, in: Niggli Marcel Alexander / Heer Marianne / Wiprächtiger Hans (édit.), *Basler Kommentar – Strafprozessordnung/Jugendstrafprozessordnung*, 3^{ème} éd., Bâle 2023.
- BOUVERAT David, art. 24 CPP, in: Jeanneret Yvan / Kuhn André / Perrier Depeursinge Camille (édit.), *Commentaire Romand – Code de procédure pénale suisse*, 2^{ème} éd., Bâle 2019.
- CARTIER Julien, *La poursuite des cybercriminels au quotidien*, in: Perrier Depeursinge Camille et al. (édit.), *Lutter contre la cybercriminalité en Suisse*, Berne 2024, 55 – 76.
- COTTIER Bertil, *Étude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet*, in: Étude du Conseil de l'Europe préparée par l'Institut suisse de droit comparé, rapport n°9, Lausanne 2015.
- D'AVILA BENDAYA Margareth, *Les mesures de surveillance des télécommunications sur Internet par les autorités en Suisse, en France et en Allemagne*, Berne 2024.
- DONATSCH Andreas / LIEBER Viktor / SUMMERS Sarah / WOHLERS Wolfgang, art. 246 CPP, *Kommentar zur Schweizerischen Strafprozessordnung StPO*, 3^{ème} éd., Zurich 2020 (cité: DONATSCH et al., art. 246 CPP).
- FURNER Mark, *First Forensic Forum Schweiz (F3-CH) Computerforensik und Computerkriminalität*, (2004) *Recht. Zeitschrift für juristische Weiterbildung und Praxis*, 210 – 212.
- HAGENSTEIN Nadine, art. 135 CP, in: Niggli Marcel Alexander / Wiprächtiger Hans (édit.), *Basler Kommentar – Strafrecht II*, 4^{ème} éd., Bâle 2019.
- HEIMGARTNER Stefan / INHELDER Elena, *Strafbarkeit dschihadistischer Propaganda*, AJP (Vol. 11) 2022, 1217 – 1232.
- HOHL-CHIRAZI Catherine, art. 246 CPP, in: Jeanneret Yvan / Kuhn André / Perrier Depeursinge Camille (édit.), *Commentaire Romand – Code de procédure pénale suisse*, 2^{ème} éd., Bâle 2019.
- JACQUEMIN Quentin, *Le droit suisse permet-il de réprimer les deepfakes ?*, in: Guillaume Florence (édit.), *La technologie, l'humain et le droit*, Berne 2023, 313 – 345.
- JAQUET-CHIFFELLE David Olivier, *Continuité de la preuve (numérique). De la scène de crime au tribunal*, in: Perrier Depeursinge Camille et al. (édit.), *Cimes et Châtiments, Mélanges en l'honneur du Professeur Laurent Moreillon*, Berne 2022, 193 – 204.
- JEANNERET Yvan / KUHN André, *Précis de procédure pénale*, 2^{ème} éd., Berne 2018.
- JOSITSCH Daniel / SCHMID Nicolas, *Schweizerische Strafprozessordnung – Praxiskommentar*, art. 246 CPP, 4^{ème} éd., Zurich / St-Gall 2023.
- JOST Lisa / NIGGLI Marcel Alexander, art. 24 CPP, in: Niggli Marcel Alexander / Heer Marianne / Wiprächtiger Hans (édit.), *Basler Kommentar – Strafprozessordnung / Jugendstrafprozessordnung*, 3^{ème} éd., Bâle 2023.
- JULEN BERTHOD Anne Valérie, art. 263 CPP, in: Jeanneret Yvan / Kuhn André / Perrier Depeursinge Camille (édit.), *Commentaire Romand – Code de procédure pénale suisse*, 2^{ème} éd., Bâle 2019.
- LAUBER Michael / MEDVED Alexander, *Terrorismusbekämpfung: Aufgabenverteilung zwischen Bund und Kantonen*, in: Fink Daniel et al. (édit.), *Kriminalität, Strafrecht und Föderalismus*, Berne 2019, 179 – 196.
- LEU Nicolas / PARVEX Denis, *Das Verbot der « Al-Quaïda » und des « Islamischen Staats ». Eine kritische Würdigung unter besonderer Berücksichtigung der Strafbarkeit djihadistischer Propaganda und der vereitelten Ausreise in ein Konfliktgebiet*, AJP (Vol. 6) 2016, 756 – 767.
- LUBISHTANI Kastriot / MONOD Hadrien, *Mesures policières de lutte contre le terrorisme*, Sécurité & Droit 1/2020, 19 – 27.

LUDWICZAK GLASSEY Maria, *Accès transfrontière aux preuves électroniques: l'avenir de l'entraide internationale en matière de cybercriminalité?*, in: Perrier Depeursinge et al. (édit.), *Lutter contre la cybercriminalité en Suisse*, Berne 2024, 117 – 130.

MÉTILLE Sylvain, intro art. 269 à 281 CPP et art. 269, 269^{bis}, 269^{ter}, 269^{quater}, 270 CPP, in: Jeanneret Yvan / Kuhn André / Perrier Depeursinge Camille (édit.), *Commentaire Romand – Code de procédure pénale suisse*, 2^{ème} éd., Bâle 2019.

MOREILLON Laurent / LUBISHTANI Kastriot, *Aspects choisis de l'incrimination du terrorisme. Étude de droit comparé suisse, allemand, français et anglais*, RPS 4/2018, 499 – 546.

MOREILLON Laurent / PAREIN-REYMOND Aude, art. 246 CPP, *Petit commentaire CPP*, 3^{ème} éd., Bâle 2025.

PAJAROLA Umberto, *Bekämpfung von Terrorismus und Organisierter Kriminalität*, Zurich / Genève 2022.

PERRIER DEPEURSINGE Camille, *CPP annoté*, 2^{ème} éd., Bâle 2020 (cité: PERRIER DEPEURSINGE, *CPP annoté*).

PLATZ Ernst, *Rechtliche Zulässigkeit von « Remote Forensic Software » in der Schweiz - Inwieweit existiert in der Schweiz eine rechtliche Grundlage für den Einsatz von "Remote Forensic Software" durch die Ermittlungsbehörden?*, (Vol. 11) 2008, 838 – 844.

POLLITT Mark et al., *A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence*, in: NIST (www.nist.gov), 2018, p. « https://www.nist.gov/system/files/documents/2018/01/10/osac_ts_0002.pdf » (consulté le 11 avril 2025) (cité: POLLITT et al.).

THORMANN Olivier / BRECHBÜHL Beat, in: Niggli Marcel Alexander / Heer Marianne / Wiprächtiger Hans (édit.), *Basler Kommentar – Strafprozessordnung/Jugendstrafprozessordnung*, art. 246 CPP, 3^{ème} éd., Bâle 2023.

TIRELLI Ludovic Adrien., *La répression pénale des consommateurs de pédopornographie à l'heure de l'Internet*, RJL (n° 35) 2008, 23 – 33.

WOHLERS Wolfgang, art. 260^{ter} CP, in: Wohlers Wolfgang / Godenzi Gunhild / Schlegel Stephan (édit.), *Schweizerisches Strafgesetzbuch – Handkommentar*, 5^{ème} éd., Berne 2024.

Documents officiels

Documents officiels rendus par les autorités suisses

Conseil fédéral, Rapport concernant les poursuites pénales en matière de cybercriminalité et l'efficacité des cantons - Commission de la politique de sécurité du Conseil national, 15 février 2022, Berne 2024 (cité: Rapport du CF, *Cybercriminalité*).

Conseil fédéral, Rapport concernant les instruments efficaces pour lutter contre l'extrémisme violent, en réponse au postulat 17.3831 Glanzmann-Hunkeler, 13 janvier 2021, Berne. (Cité: Rapport du CF, *Extrémisme*).

Conseil fédéral, Message du 22 mai 2019 concernant la loi fédérale sur les mesures policières de lutte contre le terrorisme, FF 2019 p. 4541 ss. (cité: FF 2019 4541).

Conseil fédéral, Message du 14 septembre 2018 relatif à l'arrêté fédéral portant approbation et mise en œuvre de la Convention du Conseil de l'Europe pour la prévention du terrorisme et de son Protocole additionnel et concernant le renforcement des normes pénales contre le terrorisme et le crime organisé, FF 2018 p. 6469 ss (cité: FF 2018 6469).

Conseil fédéral, Message du 18 mai 2011 relatif à l'ordonnance de l'Assemblée fédérale interdisant le groupe Al-Qaïda et les organisations apparentées, FF 2011 p. 4175 ss (FF 2011 4175).

Autres documents officiels

Counter Extremism Project, *Recommendations on Tackling Extremist Content Online*, in: Counter Extremism (www.counterextremism.com) août 2018, p. « <https://www.counterextremism.com/sites/default/files/CEP%20-%20Tackling%20Extremist%20Content%20Online.pdf> » (consulté le 14 mai 2025) (cité: CEP, *Extremist Content*).

Bureau de la défense du tribunal spécial pour le Liban, Guide pratique sur les enquêtes de la Défense dans le cadre des procès pénaux internationaux, in: Université de Limoges (www.unilim.fr), Leidschendam 2017, p. « <https://www.unilim.fr/iirco/wp-content/uploads/sites/48/2018/01/Le-Guide-des-enquetes-de-la-Defense.pdf> », (consulté le 11 avril 2025) (cité: Guide).

European Union Agency for Law Enforcement Cooperation (EUROPOL), *Facing Reality ? Law Enforcement and the Challenge of Deepfakes*, in: Europol (www.europol.europa.eu), Luxembourg 2022, p. « https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf » (consulté le 11 avril 2025) (cité: Europol, *Deepfakes*).

Pages web

Portail de la Confédération suisse, « *La Sécurité de la Suisse 2024* »: *le Service de renseignement de la Confédération publie son nouveau rapport de situation*, in: Le portail du gouvernement suisse (www.news.admin.ch), Berne 2024, p. « <https://www.news.admin.ch/fr/nsb?id=102858> » (consulté le 1^{er} avril 2025) (cité: Rapport de situation de la Confédération).