L'ENQUÊTE SOUS PSEUDONYME DANS LE CONTEXTE DE LA CYBERPÉDOPHILIE

Imane Majdoub, Khalid Atmani

Revue-IRS

Revue Internationale de la Recherche Scientifique
(Revue-IRS)
ISSN : 2958-8413
Vol. 1, No. 5, Octobre 2023

L'ENQUÊTE SOUS PSEUDONYME DANS LE CONTEXTE DE LA CYBERPÉDOPHILIE

Imane MAJDOUB

Doctorante en droit, sciences juridiques et politiques
Laboratoire de Recherches et d'Etudes Juridiques, Sociales et Judiciaires *« L.A.R.E.J.S »*
Faculté des sciences juridiques économique et sociales- Université Chouaib Doukkali- El Jadida

Directeur de Thèse : **Pr. Khalid ATMANI**, Professeur de droit pénal et de criminologie
Faculté des sciences juridiques économique et sociales- Université Chouaib Doukkali- El Jadida

Résumé : Dans un monde en perpétuelle évolution, la sécurité des mineurs face aux menaces cybernétiques notamment la cyber-pédophilie, est devenue cruciale, particulièrement à l'aune des situations des crises telles que le séisme au Maroc, où les enfants sinistrés étaient particulièrement vulnérables. Des prédateurs sexuels en ligne ont cherché à exploiter cette vulnérabilité. Cet article se plonge au cœur de cette lutte en explorant l'efficacité de l'enquête sous pseudonyme, un procédé d'investigation révolutionnaire. Nous examinons comment les avancées technologiques consolidant la cybersécurité des enfants tout en permettant aux enquêteurs de recueillir des preuves essentielles dans l'anonymat. Cet essor en matière d'investigations cybernétiques offre une nouvelle perspective pour la protection des mineurs, tout en renforçant la traque des criminels dans la sphère numérique, sans toutefois compromettre l'intégrité des procédures d'enquête et de collecte de preuves.

Mots clés : preuve numérique, cyber-pédophilie, enquête numérique, cyberprédateurs, patrouille numérique, loyauté.

Abstract: In an ever-changing world, the safety of minors in the face of cyber threats, particularly cyber-pedophilia, has become crucial, especially in light of crisis situations such as the earthquake in Morocco, where affected children were particularly vulnerable. Online sexual predators have sought to exploit this vulnerability. This article delves into the heart of this struggle by exploring the effectiveness of pseudonymous investigation, a revolutionary investigative process. We examine how technological advances are strengthening children's cybersecurity while enabling investigators to gather vital evidence anonymously. This boom in cyber investigations offers a new perspective for the protection of minors, while strengthening the hunt for criminals in the digital sphere, without compromising the integrity of investigation and evidence-gathering procedures.

Keywords: Digital evidence, cyber-pedophilia, digital investigation, cyber-predators, digital patrol, loyalty.

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.10067071

1 Introduction

Les pratiques numériques ne cessent de gagner en précocité et la cybersécurité demeure une préoccupation majeure à mesure qu'internet et les systèmes d'informations se développent, offrant de nouvelles opportunités à la criminalité, souvent transnationale, qui sait exploiter les caractéristiques de la sphère numérique telles que l'anonymat, en développant en permanence des techniques de plus en plus sophistiquées. La cyber-pédophilie est l'une des manifestations les plus visibles de cette criminalité. La cybercriminalité comprend toute activité illégale menée en ligne à l'aide d'ordinateurs ou de tout autre appareil pouvant se connecter à l'internet. Les exemples de comportements définis comme relevant de la criminalité numérique sont la cyberintimidation, le cyberharcèlement, le vol en ligne, l'usurpation d'identité et d'argent, les discours haineux, la pédopornographie, la manipulation psychologique en ligne, le harcèlement sexuel…

Plusieurs personnes sont exposées à des risques tant dans le monde en ligne que dans le monde hors ligne. Plusieurs études ont défini et mesuré la cyber-victimisation sur la base de différentes approches théoriques. Et la plupart d'entre elles se sont concentrées sur des formes spécifiques de cybercriminalité, donnant une image limitée de la victimisation. Cette forme de victimologie s'intéresse scientifiquement à tout ce qui touche à la victime au sens pénal du terme : sa personnalité, ses traits biologiques, psychologiques et moraux, ses caractéristiques socioculturelles, ses relations avec le criminel et enfin son rôle et sa contribution à la genèse du crime[1]. Notamment les mineurs victimes d'infractions.

De nombreux dangers guettent les enfants lorsqu'ils sont en ligne, la pédophilie en ligne est un crime extrêmement grave qui compromet la sécurité ainsi que le bien-être des enfants. Afin d'enrayer ce fléau, les autorités de justice utilisent différentes techniques d'enquête, comme l'infiltration numérique, la géolocalisation, l'IMSI CATCHER, afin de recueillir des preuves et de poursuivre les auteurs de ces crimes.

Face au développement croissant des TIC, les actes de pédophilie sur internet ont connu une recrudescence cruciale et considérable. La procédure pénale a dû s'adapter pour prendre en compte le développement des crimes cybernétiques. Il a été nécessaire de mettre en place des techniques d'enquête permettant la recherche des preuves numériques sur internet, y compris sur le Dark Web. Le législateur a intensifié son effort afin de réprimer certaines formes

[1] **ATMANI K., (**2022), Cours élémentaires en criminologie, 1er éd., Librairie bon coin, El Jadida, p.28.

de criminalité perpétrées via internet, en particulier celles portant atteinte aux mineurs, et a introduit la possibilité de mener des enquêtes sous pseudonyme dans les affaires de cyber-pédophilie et d'atteinte à la dignité humaine, pour concerter une cyber-confiance efficiente pour les mineurs.

Par conséquent, ces dernières années, les cas d'agressions sexuelles en ligne sur des mineurs ont émergé dans un flot incessant, obligeant les enquêteurs à innover en permanence dans les méthodes d'enquête, comme le cas d'enquête sous pseudonyme. Il s'agit d'un procédé qui vise à faciliter l'infiltration dans les réseaux criminels en ligne, permettant ainsi de recueillir des preuves cruciales tout en préservant l'anonymat et la sécurité des enquêteurs[2].

Introduite par *la loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance* qui a introduit de nouvelles dispositions habilitant certains enquêteurs à enquêter sur les atteintes aux mineurs, la traite des êtres humains sur internet et de proxénétisme sous des pseudonymes [3], en prévoyant un régime plus au moins souple que l'infiltration dans la mesure où elle ne nécessite pas une autorisation préalable d'un magistrat et n'étant pas soumis à une durée limitée[4].

La protection des mineurs sur le cyberespace s'analyse comme une question des plus pertinentes aujourd'hui, due aux progrès technologiques de plus en plus rapide et un accès facile d'internet par le mineur. Toutefois la présence du mineur et sa naïveté dans le cyberespace peuvent le transformer en proie, et le contenu des sites internet n'est pas toujours adapté nu à son âge, ni à sa sensibilité. Ce qui est anodin pour les adultes peut être perçu autrement par l'enfant. Dans la mesure où l'utilisation d'internet exige une certaine maturité, plus particulièrement la majorité des traces qu'on y laisse sont indélébiles.

Lorsque l'utilisation d'Internet est excessive, les risques sont décuplés. La raison pour laquelle, le législateur a consolidé la lutte contre certaines formes de criminalité commises par Internet notamment au préjudice de mineurs, en prévoyant l'enquête sous pseudonyme. De plus, la pornographie juvénile est devenue, dans la foulée de la popularisation d'Internet, un crime avec ses paramètres distinctifs. Ce nouveau crime n'est donc pas une adaptation d'un ancien

[2] **QUEMENER M., DALLE F., & WIERRE C.,** (2020), Quels droits face aux innovations numériques ? Législation, jurisprudences et bonnes pratiques du cyberespace - Défis et protections face aux dérives du numériques, 1er éd, Gualino Editions, Paris ? p.184.
[3] Articles 706-47-3 et 706-35-1 du Code de procédure pénale
[4] **Quéméner M.**, (2015), infiltrations numériques, *JCI, communication*, fasc. 110, n°25

crime, mais plutôt une problématique en soi que les législateurs et les intervenants de la justice ont dû comprendre puisque les façons précédentes de la combattre s'avèrent peu utiles.

Comment les évolutions technologiques peuvent-elles être utilisées pour améliorer les moyens d'investigations et de lutte contre la cyber-pédophilie, tout en concrétisant une cyber-confiance efficiente sur le cyberespace ?

Pour répondre à la question préalablement formulée, il conviendra, de prime abord, de se pencher sur la question de la consolidation du dispositif pénal en matière de cyber pédophilie, notre étude se proposera d'en expliquer la cause et soumettra un dispositif complet de lutte contre les risques d'internet afin de protéger efficacement mineurs**.** À partir de là, nous porterons notre attention en deuxième lieu sur les mesures procédurales adaptées et les modes de collecte de preuve numérique à savoir l'enquête sous pseudonyme.

2. Le socle multidimensionnel de la cyber-pédophilie

Ce sujet peut appréhender plusieurs volets, car il s'agit là d'un sujet qui monopolise de nombreux aspects et actes perpétrés sur internet qui préjudicient et ciblant principalement des mineurs, une panoplie de lois viennent consolider un socle de réglementation préexistante lorsqu'il s'agit de protéger la partie la plus vulnérable de la société, exposée aux risques imminents du cyberespace. De ce fait, en surfant sur internet, les mineurs s'exposent à des risques variés pouvant leur causer des préjudices. Pour remédier à cela, il est inévitable de cerner un corpus juridique et répressif consolidé

2.1 Les contours légaux de la pédophilie en ligne: arsenal en constante évolution

L'essor technologique peut également accroitre les risques de violences sexuelles perpétrées contre les enfants, notamment la diffusion de pornographie impliquant des enfants, principalement via Internet et de plus en plus via la téléphonie mobile[5].

Avant de se pencher sur le cadre juridique, il serait opportun de contextualiser le concept de la pornographie juvénile et plus précisément *le grooming.* On parle aussi de séduction malintentionnée des enfants, de pédopiégeage ou la manipulation psychologique des enfants, lorsqu'un adulte astucieux prend contact avec un enfant ou mineur afin de lier des rapports émotionnels avec lui dans un but de le soumettre à des abus sexuels ou à son exploitation sexuelle. On parle des *cyberprédateurs.*

[5]**AYOUBI IDRISSI H.,** (2014), Etude sur la violence sexuelle à l'encontre des enfants au Maroc, Diaaya éditions, p. 14

Ainsi, l'enquête sur l'utilisation de pseudonymes dans les réseaux pédophiles a pour but, entre autres, de distinguer entre ceux qui parlent et ceux qui agissent, en d'autres termes, les vrais cyberprédateurs dont trois profils apparaissent :

-Un prédateur qui se crée une nouvelle identité et établit un climat de confiance avec l'enfant, dans le but d'organiser une reconcentre réelle avec lui.

-Un séducteur qui agit à découvert, sans mentir sur son âge, et tente d'établir des relations avec des mineurs en ligne.

-Le pédophile qui use le monde virtuel comme moyen de communication pour atteindre ses objectifs dans le monde réel. À titre d'illustration, un éducateur qui obtient l'adresse de messagerie instantanée d'une jeune fille en la séduisant dans le monde virtuel dans le but de satisfaire ses intentions dans la réalité.

A titre d'illustration, lorsqu'on parle des prédateurs, on peut mentionner automatiquement certaines personnes malveillantes et prédateurs qui ont tenté d'exploiter la vulnérabilité des enfants sinistrés en profitant du séisme qui a durement touché le Maroc, où des images et vidéos troublantes exposant des enfants, filles et garçons, seuls dans les ruines de leur village. A cet effet, des organisations affiliées à la Plateforme Convention Droits de l'enfant (CDE) à lancer un appel contre la diffusion d'images mettant en scène ces enfants isolés parmi les décombres. Ces Organisations non gouvernementales ont discrètement créé une cellule de surveillance sur les réseaux sociaux afin de détecter les opportunistes cherchant à exploiter la situation des enfants sous couvert d'aide. Parallèlement, elles surveillent les pédophiles infiltrés dans ces réseaux. Le gouvernement a réagi rapidement en instaurant une ligne d'assistance contre la traite des êtres humains, tandis que le ministère public a créé un formulaire de signalement en ligne. Ces mesures visant à protéger les enfants sinistrés et à lutter contre toute exploitation sexuelle en ligne[6].

Toutefois, à l'échelle nationale, une panoplie de textes législatifs ont été révisés dans le but d'aligner le Maroc sur les normes internationales, notamment la Convention relative aux droits de l'enfant et le Protocole facultatif à la Convention relative aux droits de l'enfant concernant la vente d'enfants, la prostitution des enfants et la pornographie impliquant des enfants. La loi 09-08, qui concerne la protection des personnes physiques relative au traitement des données personnelles, en mettant en place la Commission Nationale du Contrôle de la protection des données personnel (CNDP). Cette commission s'efforce de promouvoir une

[6] www.h24info.ma consulté le 25/09/2023

culture de protection de la vie privée et des données personnelles des mineurs sur Internet, dans le cadre de ses initiatives de sensibilisation.

On cite également, la loi 24-03 modifiant et complétant le droit pénal de fond, qui stipule des exigences afin de promouvoir la protection pénale de l'enfant notamment contre tout acte facilité par les moyens de communication et d'information, et face aux divers risques cybernétiques, la loi 05-20 liée à la cybersécurité, et finalement la loi 103-13 relative aux violences faites aux femmes qui traite notamment les cyberviolences envers les mineures victimes.

Le Maroc a signé récemment le 2'eme protocole additionnel à la Convention du Budapest traitant la collecte transfrontalière de la preuve numérique, compte tenu du caractère transnational des crimes numériques plus particulièrement la Pornographie enfantine.

À l'échelle internationale, la France s'est engagée dans des initiatives captivantes pour lutter contre la cybercriminalité et protéger les droits des enfants. Elle a ratifié le protocole additionnel à la Convention sur la cybercriminalité (BUDAPEST), qui vise à poursuivre les actes de nature raciste et xénophobe commis via des systèmes informatiques[7]. De plus, la France a également adhéré au protocole facultatif à la Convention relative aux droits de l'enfant, s'attaquant à des problématiques sensibles telles que la vente d'enfants, la prostitution des enfants et la pornographie impliquant des enfants, une mesure adoptée par l'Assemblée générale des Nations unies en mai 2000[8].

Mais ce n'est pas tout. Depuis le 25 mai 2018, la France applique le Règlement général sur la protection des données, connu sous le nom de RGPD, qui renforce le consentement et la transparence dans l'utilisation des données. Cette réglementation innovante vise à assurer une meilleure protection des informations personnelles en faveur des mineurs.

Enfin, grâce à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui a été révisée en août 2004, la France a consacré le droit à l'oubli numérique[9] au profit des mineurs, en leur offrant ainsi la possibilité de contrôler et de supprimer les informations les concernant sur Internet. Cette avancée majeure garantit la protection de la vie privée dans l'ère numérique en permettant à chacun de façonner sa présence en ligne.

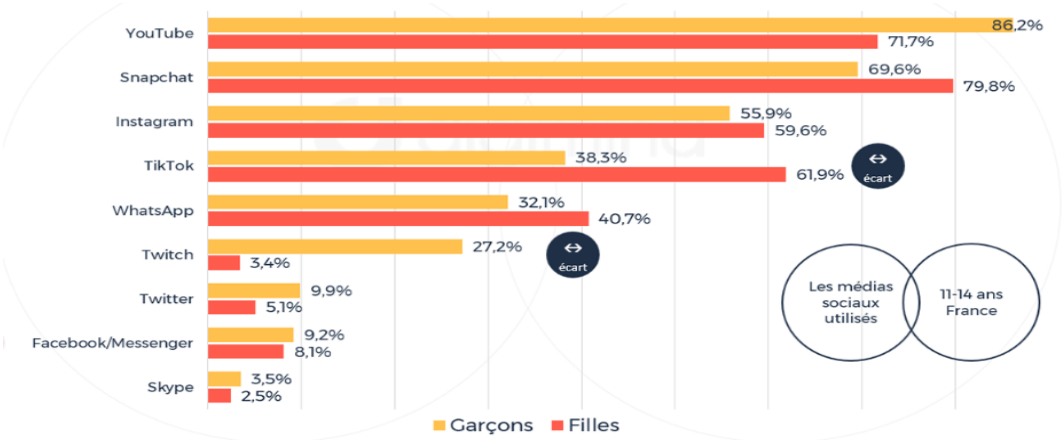
[7] Protocole signé à Strasbourg le 28 janvier 2003
[8] Ratifié par la France le 5 février 2003
[9] **LABATUT T.,** (2022), Mineurs : proposition d'un dispositif de lutte contre les risques d'internet, Lextenso. (www.actu-juridique.fr/ntic-medias-presse/mineurs-proposition-dun-dispositif-de-lutte-contre-les-risques-dinternet consulté le 03/01/2023)

La France été plus soucieuse à traiter la question de cybersécurité des mineurs et ceci à travers l'adoption de plusieurs lois en la matière, Dernièrement, quatre lois ont été adoptées afin d'encadrer certains de ces comportements nuisibles :

- En 2020, une loi pionnière a été promulguée pour encadrer l'exploitation commerciale de l'image des enfants âgés de moins de 16 ans sur les plateformes en ligne[10]. Grâce à cette loi, un pas important a été franchi pour préserver l'intégrité et la dignité des enfants dans le monde numérique en pleine expansion.
- Une deuxième loi, qui date du 2 mars 2022, a pour objectif de consolider le contrôle des parents sur les moyens d'accès à internet[11] et de combattre le harcèlement scolaire.
- Enfin, une loi récente, datée du 3 mars 2022, a été adoptée dans le but de mettre en place une certification de cybersécurité spécifiquement conçue pour les plateformes numériques accessibles au grand public.

Dès lors, Par le biais de ces quatre lois, la France a agi concrètement et efficacement pour protéger les mineurs victimes.

Figure 1 : Plateformes sociales usées par les enfants garçons et filles âgées entre 11 et 14 ans en France (%).



Source : *Génération Numérique- Enquête 2020-2021 auprès 6517 jeunes.*

La figure révèle clairement les plateformes les plus utilisées par les enfants, ce qui peut être préoccupant lorsqu'il s'agit de prévenir les risques liés à la cyber-pédophilie. Il est essentiel de

[10] L. n° 2020-1266, 19 oct. 2020, visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne

[11] L. n° 2022-300, 2 mars 2022, visant à renforcer le contrôle parental sur les moyens d'accès à internet.

noter que ces plateformes, en raison de leur popularité et de leur accessibilité, peuvent potentiellement exposer les enfants à des prédateurs en ligne.

2.2 Dispositif pénal face à la pédophilie à l'épreuve du numérique : mesures de dissuasion renforcées

Consciente des risques accrus pour les mineurs liés aux nouveaux moyens de communication, la législation a réagi de manière appropriée. Le législateur a ainsi pris en compte la dangerosité de ces technologies envers les enfants et soutient que les sanctions pénales prévues seront alourdies pour mieux lutter contre la cybercriminalité si les crimes et délits prévus par le Code pénal sont commis sur les réseaux de télécommunications. **L'article 497** du code pénal marocain vise à réprimer la corruption de la jeunesse et la prostitution en imposant des sanctions sévères. Selon cet article, toute personne qui encourage, favorise ou facilite la débauche ou la prostitution de mineurs âgés de moins de dix-huit ans peut être condamnée à une peine d'emprisonnement allant de deux à dix ans, ainsi qu'à une amende variante entre vingt mille et deux cent mille dirhams.

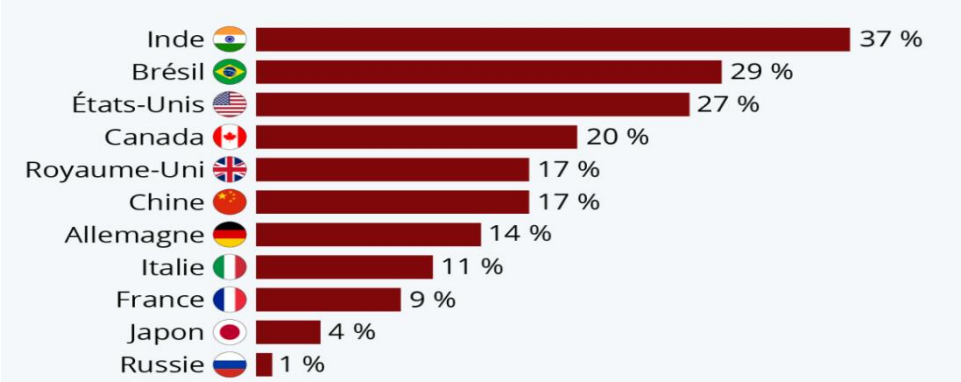
L'article 503-2 du code pénal marocain prévoit des peines pour réprimer la pédopornographie. Selon cet article, toute personne qui provoque, incite ou facilite l'exploitation d'enfants âgés de moins de dix-huit ans dans des représentations pornographiques, que ce soit par des actes sexuels réels, simulés, perçus ou par des représentations des organes sexuels d'un enfant à des fins sexuelles, est passible d'une peine d'emprisonnement d'un an à cinq ans, ainsi que d'une amende allant de dix mille à un million de dirhams. De plus, la même peine s'applique à quiconque produit, diffuse, publie, importe, exporte, expose, vend ou détient des matières pornographiques similaires, y compris par le biais des moyens de télécommunication.

Pour ce qui est cadre légal et règlementaire, le législateur français a concrétisé **un arsenal législatif sanctionnant des actes considérés comme étant préjudiciables pour mineurs.** Toutefois, le Code pénal prévoit des dispositions spécifiques pour punir non seulement la diffusion d'images ou de représentations pornographiques impliquant des mineurs, mais également le fait qu'un message à caractère pornographique soit vu ou perçu par un mineur. L'article 227-24 du Code pénal français prévoit que toute personne qui fabrique, transporte ou diffuse, par tout moyen et quel que soit le support utilisé, un message à caractère violent, pornographique ou susceptible de porter gravement atteinte à la dignité humaine, ainsi

que toute personne qui en fait commerce, est passible d'une peine d'emprisonnement de 3 ans et d'une amende de 75 000 euros.

Cette disposition impose une obligation de résultat aux éditeurs de contenus afin de veiller à ce que les mineurs ne puissent pas accéder à des contenus préjudiciables répandus sur Internet ou sur les téléphones mobiles.

Figure 2 : Part des parents déclarant que leur enfant a été victime de cyberharcèlement en (%)



Source : IPSOS, *Enquête menée en 2018 auprès de 20 793 adultes dans 28 pays*

Illustration jurisprudentielle :

Le 22 février 2005, la Cour d'appel de Paris a rendu un jugement confirmant la condamnation des éditeurs de contenus pornographiques. L'un des éditeurs a été condamné à une peine de trois mois d'emprisonnement avec sursis et une amende de 3000 euros, tandis que l'autre a été condamné à une peine de six mois d'emprisonnement avec sursis et une amende de 3000 euros. Les deux accusés ont été reconnus coupables de n'avoir pas empêché l'accès de mineurs à leurs sites, même s'ils avaient mis en place des avertissements à l'écran et demandé aux internautes de confirmer leur majorité. Malgré ces mesures préventives, les mineurs ont pu accéder aux contenus inappropriés. Cette décision de justice souligne l'importance de prendre des mesures efficaces pour protéger les mineurs en ligne et la responsabilité des éditeurs de contenus pour prévenir l'accès des mineurs à des contenus préjudiciables.[12]

En ce qui concerne les viols commis sur des mineurs, *l'article 222-24 alinéa 8 du Code pénal français* dispose que le viol est passible d'une peine de réclusion criminelle de 20 ans

[12] CA Paris, 11echambre A, 22 février 2005, B.G.,J.-M. société New Video Production c./ le ministère public, Juris-data,n° 2005-27529

dans les cas suivants : lorsque la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation d'un réseau de télécommunications pour la diffusion de messages à destination d'un public non déterminé. On cite à cet effet les atteintes sexuelles commises sur des mineurs[13] victimes, les cas de proxénétisme facilité par l'utilisation des moyens de télécommunications[14] ou encore des cas de corruption des mineurs, au moment où ce dernier a été mis en contact avec le délinquant par le biais d'Internet[15]. Dans cette perspective, le code pénal sanctionne également dans son article 321-1 le recel des images de pornographie enfantine.

On déduit que l'arsenal pénal existe, mais les enjeux subsistent dans sa mise en œuvre vu que le crime cybernétique s'organise chaque jour davantage. Les outils procéduraux évoluent mais l'utilisation massive des nouvelles technologies par les jeunes facilite la corruption des mineurs. Il y a donc un besoin urgent de prévoir des mesures d'enquêtes spéciales en dotant les enquêteurs des armes juridiques pour lutter contre la pédo-criminalité en ligne et d'éviter l'impunité des cyberprédateurs. C'est le cas de *l'enquête sous pseudonyme.*

3 Patrouille numérique et enquête sous pseudonyme comme armes secrètes de la justice

La virtualité inhérente au cyberespace permet d'échanger du matériel non tangible, donc plus difficilement saisissable pour les policiers. Pour répondre aux techniques toujours plus sophistiquées et ingénieuses utilisées par les délinquants pour échapper à l'identification et à la collecte de preuves, le champ d'application de l'enquête sous pseudonyme a été élargi progressivement. Mais, cette investigation cybernétique peut dans certains cas, être freinée par certaines limites considérables.

3.1 Champ d'application et spécificités de l'enquête sous pseudonyme

Selon l'article 230-46 du Code de procédure pénale français, qui s'inspire de la loi n° 2019-222 du 23 mars 2019 sur la programmation et la réforme de la justice, cette procédure est applicable aux infractions liées aux atteintes aux systèmes de traitement automatisé de données. Elle est spécifiquement limitée aux cas de crimes et de délits punis d'une peine d'emprisonnement commis par le biais des communications électroniques.[16].

Les officiers ou agents de la police judiciaire qui sont autorisés peuvent utiliser cette mesure pour surveiller les personnes suspectées de commettre des infractions par le biais de

[13] Article 227-26 al. 4 du Code pénal
[14] Article 225-7 al. 10
[15] Article 227-22 du Code pénal
[16] **SPITZ Bernard,** (2021) le droit pénal à l'épreuve des cyberattaques, rapport club des juristes, Paris, p.72

communications électroniques. Ils ont la possibilité de se faire passer pour l'un des "coauteurs, complices ou receleurs" des suspects, de participer aux échanges électroniques sous un pseudonyme, d'entrer en contact avec les suspects et de recueillir des éléments de preuve et des données sur ces individus.

Le code de procédure pénale marocain a en effet, connait une évolution notable en matière d'investigation cybernétique, de ce fait, un nouveau cadre législatif a été décrypté, c'est bel bien l'infiltration numérique prévue suite aux dispositions des **articles 82-3-1 et 82-3-6** du projet du code de procédure pénale marocain. Dès lors, si les besoins de l'enquête ou de l'investigation concernant l'un des crimes ou délits relevant de l'article 108 du projet de code de procédure pénale marocain le requièrent, le ministère public a la possibilité d'autoriser, sous leur surveillance respective, une opération d'infiltration.[17]

Mais, il ne faut pas confondre le procédé d'infiltration et celui d'enquête sous pseudonyme qui se concordent fortement. Dans la mesure où l'infiltration permet une exonération de responsabilité pénale pour l'agent infiltré, ce qui n'est pas le cas pour l'enquête sous pseudonyme.

De ce fait, une panoplie de types d'actions qui sont admissibles dans le cadre d'une cyber-patrouille, on cite à cet effet :

- Prendre part à des échanges électroniques, y compris avec les individus potentiellement impliqués dans ces infractions.
- Collecter ou conserver par ce moyen des données relatives aux personnes pouvant être les auteurs de ces infractions, ainsi que tout élément de preuve.
- Sous réserve de l'autorisation préalable du juge d'instruction compétent, obtenir tout contenu, produit, substance, échantillon ou service, même illicite, ou répondre à une demande explicite de contenus illicites. [18]

L'enquête sous pseudonyme est menée de deux manières distinctes :

- Une investigation dite "d'initiative" consiste à ce que les agents ou les officiers s'infiltrent délibérément dans un réseau informatique où ils ont connaissance de la commission d'infractions liées à la pédopornographie, dans le but d'identifier les coupables.

[17] **BENSELIMANE A.**, le crime cybernétique en droit marocain : étude critique et comparative, 1er éd. Dar al Aman , Rabat, p.172

[18] **Takoudju S., Freslon J. (2021),** les règles de droit face à la pédopornographie, in *village de la justice. (www.village-justice.com/articles/pedopornographie,39162.html* consulté le 30/12/2022)

- Dans le cas de reprise de profil de la victime, l'agent ou l'officier de police judiciaire utilise le pseudonyme de la victime pour reprendre contact avec l'auteur d'une infraction, dans le but de l'identifier. L'enquêteur se présente alors de manière vraisemblable en tant que mineur, en prenant la place de la victime sur tous les réseaux de communication où l'auteur intervient. Cela est effectué avec le consentement des parents du mineur victime.

Cependant, il convient de souligner que l'enquête sous pseudonyme est généralement autorisée uniquement pour un ensemble restreint d'infractions spécifiquement énumérées par la loi. Ces infractions incluent notamment la traite des êtres humains, le proxénétisme et les atteintes en bande organisée à un système de traitement automatisé de données (STAD) à caractère personnel mis en œuvre par l'État, terrorisme, Criminalité organisée…). Mais cette enquête peut être utilisée également dans le cadre où un mineur est en danger comblant une incitation du mineur à commettre une infraction liée aux produits stupéfiants ou à la consommation excessive ou encore habituelle des boissons alcooliques … corruption, propositions sexuelles à mineur de 15 ans, pédopornographie, en cas de recourir à la prostitution des mineurs.

3.2 Exploration des limites des enquêtes sous pseudonyme : Les controverses entourant la déloyauté de la preuve

L'enquête sous pseudonyme offre aux officiers et agents de police judiciaire une méthode d'investigation proactive grâce à sa flexibilité. A peine de nullité, il est essentiel que ces actes d'enquête ne puissent pas inciter à la commission d'infractions afin de préserver le principe fondamental de la loyauté de la preuve. Ainsi, leur mise en œuvre doit respecter scrupuleusement cette exigence, sans compromettre le fondement essentiel du procès équitable. De ce fait, la loyauté de la preuve dans le cadre de l'enquête sous pseudonyme peut se révéler comme étant un revers quant à l'admissibilité et la recevabilité de cette technique d'investigation.

Le respect du principe de loyauté et l'interdiction de provoquer délibérément des infractions sont des limites essentielles encadrant l'utilisation de cette méthode de preuve numérique. Bien que ces enquêtes puissent permettre la constatation des infractions et la sollicitation de preuves, il est strictement interdit de les utiliser dans le but d'encourager la commission d'une infraction. Par conséquent, bien que les enquêteurs soient autorisés à participer à des échanges électroniques avec un internaute majeur sous un pseudonyme, ils ne

peuvent en aucun cas proposer des contenus illicites sans une demande préalable explicite, sous peine de prononcer la nullité de la procédure.[19]

L'enquête sous pseudonyme peut avoir un impact sur la loyauté de la preuve numérique dans le sens où elle soulève certaines questions et préoccupations liées à l'authenticité et à la fiabilité des preuves recueillies. Voici quelques points importants à considérer :

- ✓ **Authentification des preuves :** Lors de l'enquête sous pseudonyme, les enquêteurs peuvent interagir avec les suspects en utilisant des identités fictives. Cela peut poser des défis en ce qui concerne l'authentification des preuves numériques recueillies. Il est crucial de pouvoir prouver de manière convaincante que les conversations, les images ou les autres éléments de preuve ont bien été obtenus dans le cadre de l'enquête légitime et qu'ils n'ont pas été falsifiés ou altérés.
- ✓ **Intégrité des preuves :** Lorsqu'une enquête est menée sous pseudonyme, il est essentiel de garantir l'intégrité des preuves numériques collectées. Cela signifie que les enquêteurs doivent être en mesure de démontrer que les preuves n'ont pas été manipulées, altérées ou corrompues pendant le processus de collecte. Des protocoles stricts doivent être suivis pour préserver l'intégrité des données numériques et assurer qu'elles peuvent être présentées devant un tribunal de manière crédible.
- ✓ **Confidentialité des méthodes d'enquête :** L'enquête sous pseudonyme nécessite souvent que les enquêteurs gardent secrètes leurs méthodes et techniques spécifiques. Cela peut rendre difficile pour la défense d'examiner ou de remettre en question ces méthodes lors du procès. L'opacité entourant les enquêtes sous pseudonyme peut soulever des préoccupations quant à la transparence et à l'équité de la procédure judiciaire.

Il est important de noter que les tribunaux peuvent évaluer la loyauté de la preuve numérique recueillie lors d'une enquête sous pseudonyme en fonction de plusieurs facteurs, tels que la conformité aux lois et procédures, la fiabilité des méthodes d'enquête utilisées, la préservation de l'intégrité des preuves et la garantie des droits des accusés.

Application jurisprudentielle :

Dans **un arrêt du 11 mai 2006**[20], la Cour de cassation a déclaré la nullité de la procédure pour atteinte au principe de la loyauté des preuves et au droit à un procès équitable,

[19] **CECyF – Cyberlex,** (2018), la procédure pénale face aux évolutions de la cybercriminalité et du traitement de preuve numérique, p.12, rapport disponible sur www.Cyberlex.org et www.CECyF.fr)
[20] Cour de Cassation, Chambre criminelle, du 11 mai 2006, 05-84.837 (disponible sur www.legifrance.gouv.fr)

conformément à l'article 6 de la Convention européenne des droits de l'homme et à l'article préliminaire du code de procédure pénale. Cette décision fait suite à la constatation que la provocation à la commission d'une infraction, telle que se connecter sur internet en se faisant passer pour un mineur en vue de rechercher des relations sexuelles, est une provocation au délit de transmission de fichiers pédophiles[21].

En conséquence, l'utilisation d'une telle méthode est considérée comme déloyale, ce qui rend les éléments de preuve ainsi obtenus irrecevables devant un tribunal. Cette décision met en évidence l'importance du respect du principe de loyauté de la preuve et du droit à un procès équitable, et souligne que les actions de provocation par des agents de police ou des intermédiaires ne peuvent pas être utilisées pour étayer l'accusation et poursuivre les présumés coupables.

Un autre arrêt qui illustre le cadre d'une preuve déloyale par la provocation, qui date le 27 février 2014[22] rendu par la chambre de l'instruction de la Cour d'Appel, Paris. En l'espèce, Deux particuliers, agissant de leur propre initiative, ont provoqué la commission d'une infraction en se faisant passer pour des agents des services secrets. Par conséquent, il est nécessaire de limiter et encadrer l'intervention d'agents infiltrés, même dans le cadre de la répression et de l'identification des auteurs de cyber-pédophilie ainsi que des individus mettant en danger la sécurité des mineurs sur Internet. Même si l'intérêt public est en jeu, cela ne justifie pas l'utilisation de preuves recueillies à la suite d'une provocation policière.

Un autre point qui peut constituer une limite à la recevabilité de la preuve pénale numérique concerne les preuves obtenues par des particuliers ordinaires qui ne font pas partie du corps judiciaire. Il s'agit de personnes privées qui s'assignent pour mission de traquer et identifier ceux qu'elles considèrent comme des auteurs d'infractions sexuelles sur Internet.

Dans cette perspective, le contournement des règles de procédure est attentivement scruté par la Cour de cassation. En effet, l'Assemblée plénière a pu juger que seul peut être prescrit « *le stratagème qui, par un* ***contournement ou un détournement d'une règle de procédure*** *a pour objet ou pour effet de vicier la recherche de la preuve* ***porte atteinte à l'un des droits essentiels ou à l'une des garanties fondamentales de la personne suspectée ou poursuivie*** ». Elle affirme notamment que « *si la provocation, par un agent de l'autorité publique, à la commission de l'infraction, constitue une violation du principe de loyauté de la*

[21] **QUÉMÉNER M.**, (2016), les nouvelles techniques d'infiltration, enquete sous pseudonyme : législations et pratique, ADIJ, p.14

[22] CA Paris, P. 7, 1re ch. instr., 27 févr. 2014, nos 2013/02604 et 2013/07319

preuve, le fait qu'il recoure à un stratagème tendant à la constatation d'une infraction ou l'identification de ses auteurs ne constitue pas, en soi, une atteinte à ce principe » **(Affaire Benzema, AP, 9 décembre 2019 n°18-86767[23]).**

Ainsi, les juridictions examinent deux conditions pour déterminer si une preuve est effectivement déloyale ou non :

- Une condition de fond : Les juridictions vérifient si les enquêteurs ont adopté un comportement actif ou passif et s'ils ont exercé une influence susceptible d'encourager la commission de l'infraction. Si les enquêteurs ont provoqué ou incité délibérément l'auteur présumé à commettre l'infraction, cela peut être considéré comme déloyal.
- Une condition procédurale ou de forme: Les juridictions examinent également si le mode de preuve a fait l'objet d'un débat contradictoire dans un but de garantir l'effectivité des droits de la défense.

En résumé, la recevabilité des preuves pénale numérique obtenues par des particuliers privés peut être remise en question. Les tribunaux évalueront la compétence, la légitimité, le respect des droits fondamentaux, la collaboration avec les autorités compétentes et le respect des procédures légales renforcent la crédibilité et la recevabilité des preuves, pour déterminer si ces preuves sont admissibles dans le cadre d'une procédure judiciaire.

4 Conclusion

On déduit que l'intervention du législateur a permis de doter les enquêteurs et les magistrats instructeurs d'outils probatoires appropriés pour faire face aux défis posés par les nouvelles technologies. L'enquête sous pseudonyme constitue l'un de ces outils, offrant des possibilités d'investigation efficaces tout en préservant les droits et la sécurité des personnes impliquées dans le processus.

Il est effectivement plus judicieux de bien encadrer le champ d'application des enquêtes numériques de ce type dans le cadre des investigations, lorsque la commission des infractions portant préjudice aux mineurs est facilitée par les TIC, afin de renforcer les garanties en lien avec cette technique, sur la vie privée, et dans une perspective de concerter une confiance numérique dans le cyberespace.

[23] Cour de cassation, Assemblée plénière, 9 décembre 2019, 18-86.767. (www.legifrance.gouv.fr/juri/id)

Aujourd'hui, les cybercriminels exploitent de plus en plus Internet en tant que territoire propice à la commission d'infractions, notamment dans le domaine de la pédophilie. Face à cette réalité, le pouvoir judiciaire est tenu de s'adapter à cette nouvelle forme de criminalité et, éventuellement, d'utiliser les mêmes méthodes. Il n'est plus approprié de considérer les techniques d'enquête classiques comme opposées aux techniques dites spéciales, car ces nouvelles méthodes sont devenues indispensables pour les enquêteurs. De ce fait, on peut dire que les mécanismes actuels ont vocation, à moyen terme, à lutter efficacement contre ces risques cybernétiques, mais malgré les efforts fournis, le cadre juridique actuel laisse subsister encore des failles. Une protection des victimes uniquement par un durcissement de la répression est vain, le cadre procédural à l'épreuve des avancées technologiques doit être renforcée et consolidée.

REFERENCES

[1] ATMANI K., (2022), Cours élémentaires en criminologie, 1er éd., Librairie bon coin, El Jadida.

[2] AYOUBI IDRISSI H., (2014), Etude sur la violence sexuelle à l'encontre des enfants au Maroc, Diaaya éditions, 105P.

[3] BENSELIMANE A. (2017), le crime cybernétique en droit marocain : étude critique et comparative, 1er éd. Dar al Aman , Rabat. 286P

[4] CECyF – Cyberlex, (2018) La Procédure Pénale Face Aux Evolutions De La Cybercriminalité Et Du Traitement De La Preuve Numérique, 46P. Rapport disponible sur www.Cyberlex.org et www.CECyF.fr)

[5] LABATUT T., (2022), Mineurs : proposition d'un dispositif de lutte contre les risques d'internet, Lextenso. (www.actu-juridique.fr/ntic-medias-presse/mineurs-proposition-dun- dispositif-de-lutte-contre-les-risques-d 'Internet consulté le 03/01/2023)

[6] QUEMENER M., DALLE F., & WIERRE C., (2020), Quels droits face aux innovations numériques ? Législation, jurisprudences et bonnes pratiques du cyberespace - Défis et protections face aux dérives du numériques, 1er éd, Gualino Editions, Paris. 232P

[7] QUÉMÉNER M., (2016), Nouvelles techniques d'infiltrations, enquête sous pseudonyme: législations et pratique, ADIJ, 16P.

[8] QUÉMÉNER M., (2015), infiltrations numériques, JCI, communication, fasc. 110, n°25

[9] SPITZ Bernard, (2021) Le Droit Pénal À L'épreuve Des Cyberattaques, rapport du club des juristes, Paris. 46P

[10] TAKOUDJU S., FRESLON J. (2021), Les Règles De Droit Face À La Pédopornographie, in village de la justice. (www.village-justice.com/articles/pedopornographie,39162.html consulté le 30/12/2022)

[11] Dahir N° 1-59-413 Du 28 Joumada Ii 1382 (26 Novembre 1962) Portant Approbation Du Texte du Code Pénal Marocain .
[12] Dahir n° 01-02-255 du 3 octobre 2002 portant loi n° 22-01 relative au code de procédure pénal publié au B.O n° 5078 du 30 janvier 2003
[13] Dahir n° 1-03-207 du 11 novembre 2003 portant promulgation de la loi n° 24-03 modifiant et complétant le Code pénal.
[14] L. n° 2020-1266, 19 oct. 2020, visant à encadrer l'exploitation commerciale de l'image d'enfants de moins de seize ans sur les plateformes en ligne
[15] L. n° 2022-300, 2 mars 2022, visant à renforcer le contrôle parental sur les moyens d'accès à internet.
[16] Cour de Cassation, Chambre criminelle, du 11 mai 2006, 05-84.837 (disponible sur www.legifrance.gouv.fr)
[17] CA Paris, P. 7, 1re ch. instr., 27 févr. 2014, nos 2013/02604 et 2013/07319
[18] CA Paris, 11echambre A, 22 février 2005, B.G.,J.-M. société New Video Production c./ le ministère public, Juris-data,n° 2005-27529
[19] Cour de cassation, Assemblée plénière, 9 décembre 2019, 18-86.767. (www.legifrance.gouv.fr/juri/id)
[20] www.h24info.ma consulté le 25/09/2023