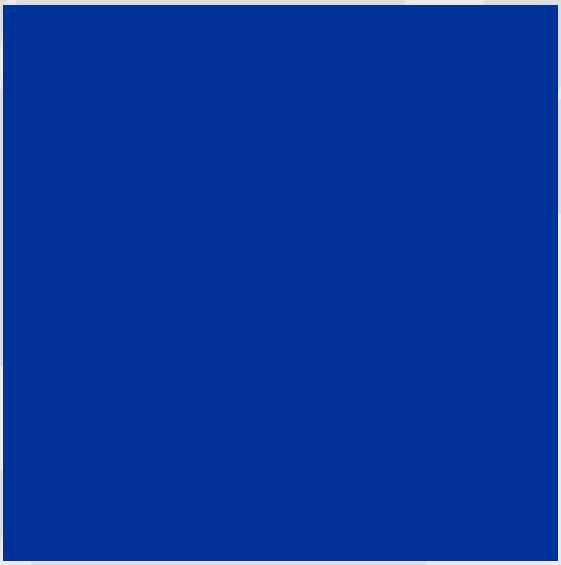
ASPECTS DE LA SÉCURITÉ SOCIALE

Mesures de protection des enfants et des jeunes face aux cyber-délits sexuels

Rapport de recherche nº 16/22



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Département fédéral de l'intérieur DFI
Bundesamt für Sozialversicherungen BSV
Office fédéral des assurances sociales OFAS

L'Office fédéral des assurances sociales publie dans sa série « Aspects de la sécurité sociale » des travaux conceptuels et des rapports de recherche ou d'évaluation sur des sujets d'actualité dans le domaine de la sécurité sociale pour les rendre accessibles au grand public et stimuler la discussion. Les conclusions et les recommandations présentées par les auteurs ne reflètent pas forcément l'opinion de l'Office fédéral des assurances sociales.

Auteurs:
Stefano Caneppele, Christine Burkhardt, Amandine Da Silva, Lachlan Jaccoud, Fabian Muhly, Sandra Ribeiro
Ecole des sciences criminelles
Université de Lausanne
Bâtiment Batochime
CH-1015 Lausanne
Tél. +41 (0)21 692 46 42 (direct), +41 (0)21 692 46 00 (secrétariat)
Courriel: stefano.caneppele@unil.ch
Internet: www.unil.ch/esc

Renseignements:
Office fédéral des assurances sociales
Effingerstrasse 20
CH-3003 Berne

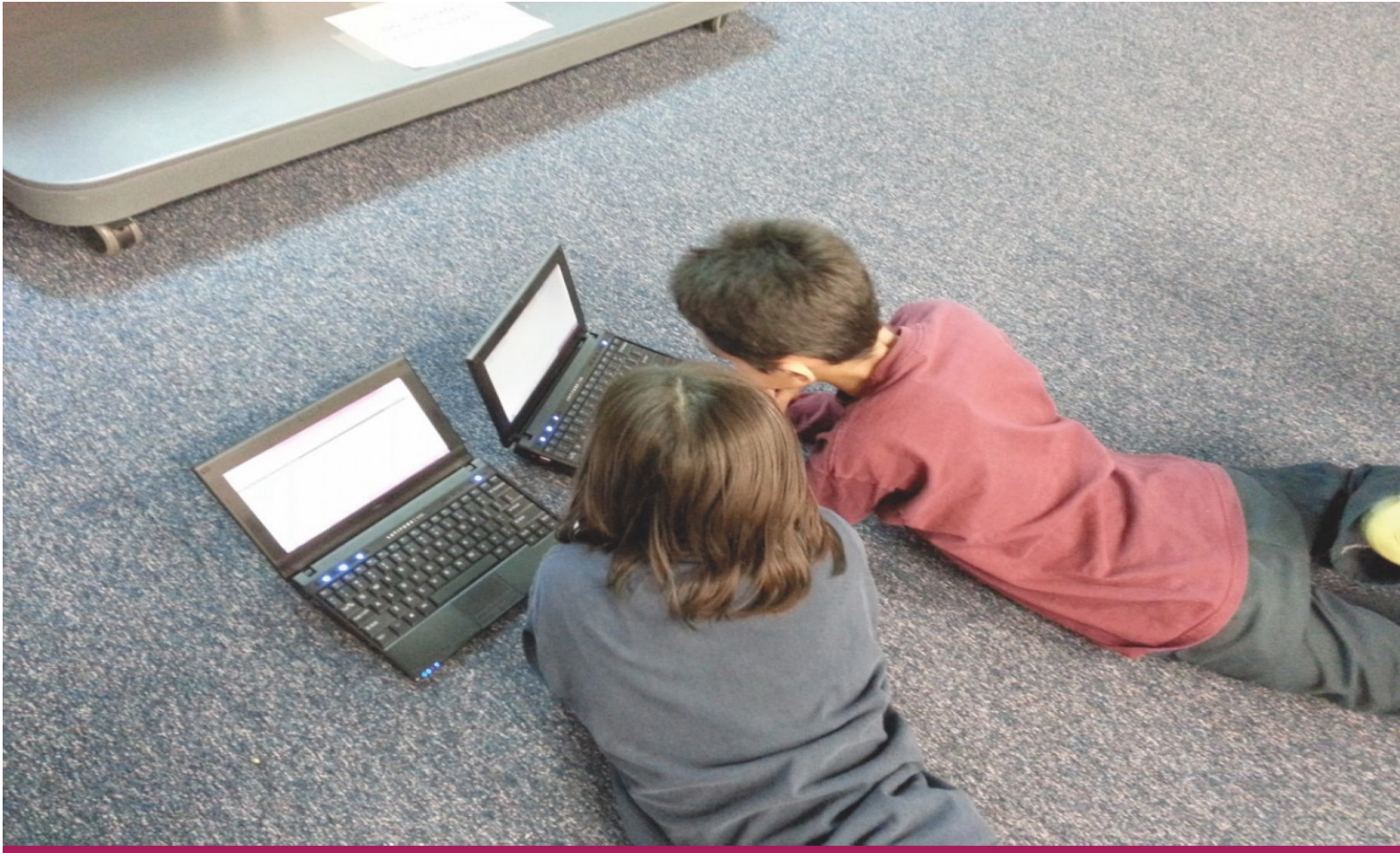
Martina Gregori-Robbiani
Domaine Famille, générations et société
Tél. +41 (0)58 485 07 80
Courriel: martina.gregori-robbiani@bsv.admin.ch

Yvonne Haldimann
Domaine Famille, générations et société
Tél. +41 (0)58 462 90 98
Courriel: yvonne.haldimann@bsv.admin.ch

ISSN:
1663-4659 (rapport électronique)
1663-4667 (version imprimée)

Diffusion:
OFCL, vente des publications fédérales, CH-3003 Berne
www.publicationsfederales.admin.ch

Numéro de commande:
318.010.16/22F



Mesures de protection des enfants et des jeunes face aux cyber-délits sexuels

Projet J21_02

Etude sur mandat de l'Office fédéral des assurances sociales

Stefano Caneppele
Christine Burkhardt
Amandine Da Silva
Lachlan Jaccoud
Fabian Muhly
Sandra Ribeiro

Juillet 2022

UNIL | Université de Lausanne
Ecole des sciences criminelles

Avant-propos de l'Office fédéral des assurances sociales

Le postulat Rosmarie Quadranti [Heinz Siegenthaler] (19.4111) « Protéger les enfants et les jeunes et empêcher les criminels de les inciter ou de les forcer à se livrer à des actes sexuels sur eux-mêmes en se filmant avec leur téléphone » charge le Conseil fédéral d'examiner quelles mesures juridiques, techniques ou autres permettraient d'empêcher que les enfants et les jeunes ne soient incités ou forcés à réaliser des enregistrements relevant de la pédopornographie par des adultes qui gagnent leur confiance pour les exploiter sexuellement. Outre des mesures juridiques et techniques, le présent rapport se penche sur des mesures préventives et policières. L'Office fédéral des assurances sociales, qui chapeaute le projet, a confié à l'université de Lausanne un mandat de recherche pour l'élaboration des bases.

L'étude décrit le contexte suisse et le droit en vigueur ainsi que l'état des connaissances sur les quatre cyber-délits sexuels traités : la production et la distribution de matériel pédopornographique via Internet, le *cyber grooming* (ou pédopiégeage), la sextorsion et la retransmission en direct (*live streaming*) d'abus sexuels sur des enfants. Des rapports de recherche et des statistiques montrent que de tels actes sont fréquents en Suisse. Il s'avère cependant difficile de dégager des tendances et de recueillir des données probantes sur les victimes, les auteurs et leurs façons de procéder, d'une part à cause du manque de connaissances à ce sujet, d'autre part en raison de l'évolution (technologique) rapide dans ce domaine. La présente étude décrit les principales caractéristiques de ces cas et les cinq catégories de plateformes que les auteurs de cyber-délits sexuels utilisent le plus souvent.

En Suisse, la protection de l'enfance et les poursuites pénales relèvent principalement de la compétence des cantons. La Confédération a un rôle subsidiaire et assure des tâches spécifiques, comme la collaboration et la coopération internationale avec Interpol et Europol. Les organisations privées et les entreprises de télécommunications s'impliquent également beaucoup dans ce domaine. De fait, de nombreuses mesures juridiques, techniques, préventives et policières existent déjà pour répondre à cette problématique.

À partir des lacunes qu'elle a identifiées, l'équipe de projet formule dix recommandations destinées à améliorer la protection des enfants et des jeunes contre les délits d'ordre sexuel, aux cinq niveaux suivants : 1) encouragement de la recherche scientifique, 2) renforcement de la coordination et de la collaboration entre acteurs, 3) esprit d'innovation dans les mesures de prévention, 4) atteinte des groupes cibles grâce à une approche globale et 5) soutien des évaluations scientifiques pour créer et améliorer de bonnes pratiques.

Les résultats du rapport de recherche sont intégrés au rapport du Conseil fédéral en réponse au postulat Quadranti (19.4111). Pour les principaux acteurs, ils constituent par ailleurs une base importante en vue de concevoir ou de développer des mesures appropriées, et ainsi de protéger efficacement les enfants et les jeunes contre les actes d'ordre sexuel en ligne.

Astrid Wüthrich
Responsable du domaine Famille, générations et société

Vorwort des Bundesamts für Sozialversicherungen

Das Postulat Rosmarie Quadranti [Heinz Siegenthaler] (19.4111) «Kinder und Jugendliche vor der Handykamera nicht alleine lassen. Täter stoppen, die Kinder dazu anleiten oder erpressen, sexuelle Handlungen an sich selbst vorzunehmen», beauftragt den Bundesrat zu prüfen, welche rechtlichen, technischen und sonstigen Massnahmen nötig sind, damit Kinder und Jugendliche nicht zur Herstellung von kinderpornografischem Material angeleitet oder erpresst werden können von Erwachsenen, die sich ihr Vertrauen erschleichen, um sie dann sexuell auszubeuten. Neben rechtlichen und technischen werden im vorliegenden Bericht präventive und polizeiliche Massnahmen untersucht. Das federführende Bundesamt für Sozialversicherungen hat zur Erarbeitung der Grundlagen einen Forschungsauftrag an die Universität Lausanne vergeben.

Die Studie beschreibt den Schweizer Kontext und das geltende Recht sowie den Wissensstand zu den vier behandelten Cyber-Sexualdelikten: Herstellung und Verbreitung von Darstellungen sexueller Handlungen mit Kindern im Internet, Cybergrooming, Sextortion und Live-Streaming von sexuellem Missbrauch an Kindern. Forschungsberichte und Statistiken zeigen, dass sie in der Schweiz verbreitet sind. Trends aufzuzeigen und schlüssige Daten zu den Opfern, den Täterinnen und Tätern und ihrer Vorgehensweise zu erhalten, erweist sich jedoch als schwierig, einerseits aufgrund von Wissenslücken und andererseits wegen der raschen (technologischen) Entwicklungen in diesem Bereich. Die vorliegende Studie zeigt die wichtigsten Merkmale dieser Fälle und die fünf Kategorien von Plattformen, die von der Täterschaft von Cyber-Sexualdelikten am häufigsten verwendet werden.

In der Schweiz fallen der Kinderschutz und die Strafverfolgung hauptsächlich in die Zuständigkeit der Kantone. Der Bund handelt subsidiär bzw. übernimmt spezifische Aufgaben, beispielsweise die Zusammenarbeit und die internationale Kooperation mit Interpol und Europol. Auch private Organisationen und Telekommunikationsunternehmen leisten einen wichtigen Beitrag zur Bekämpfung. Daraus ergeben sich zahlreiche rechtliche, technische, präventive und polizeiliche Massnahmen, mit denen die Problematik bereits heute angegangen wird.

Aufgrund der identifizierten Lücken formuliert das Forschungsteam zur Verbesserung des Schutzes von Kindern und Jugendlichen vor Cyber-Sexualdelikten zehn Empfehlungen auf folgenden fünf Ebenen: 1) Förderung der wissenschaftlichen Forschung, 2) Verstärkung der Koordination und Zusammenarbeit der Akteure, 3) Präventionsmassnahmen: Offenheit für Innovation 4) Erreichen der Zielgruppen durch ganzheitlichen Ansatz und 5) Förderung von wissenschaftlichen Evaluationen zur Verbesserung und Etablierung guter Praxis.

Die Ergebnisse des Forschungsberichts fliessen in den bundesrätlichen Bericht zum Postulat Quadranti (19.4111) ein. Sie sind zudem eine wichtige Grundlage für die zentralen Akteure, um entsprechende Massnahmen zu erarbeiten bzw. weiterzuentwickeln und Kinder und Jugendliche so wirksam vor sexuellen Übergriffen im Netz zu schützen.

Astrid Wüthrich
Leiterin Geschäftsfeld Familie, Generationen und Gesellschaft

Premessa dell'Ufficio federale delle assicurazioni sociali

Il postulato Rosmarie Quadranti (Heinz Siegenthaler) 19.4111 «Non lasciare bambini e adolescenti da soli davanti alla videocamera del cellulare. Fermare chi li induce a compiere atti sessuali su se stessi adescandoli o ricattandoli» chiede al Consiglio federale di verificare quali misure giuridiche, tecniche o di altro tipo siano necessarie per impedire che bambini e adolescenti possano essere adescati o ricattati per la produzione di materiale pedopornografico da parte di adulti che carpiscono la loro fiducia per poi sfruttarli sessualmente. Il presente rapporto analizza, oltre a misure giuridiche e tecniche, anche misure preventive e di polizia. In qualità di organo responsabile in materia, l'Ufficio federale delle assicurazioni sociali ha conferito all'Università di Losanna un mandato di ricerca per l'elaborazione delle basi necessarie per l'adempimento dell'incarico.

Lo studio descrive il contesto svizzero e il quadro giuridico applicabile nonché lo stato delle conoscenze disponibili su quattro reati sessuali online: produzione e diffusione di rappresentazioni di atti sessuali con minori su Internet, cibergrooming, sextortion e live streaming di abusi sessuali su minori. Dall'analisi di vari rapporti di ricerca e statistiche emerge che tali reati sono diffusi in Svizzera. È tuttavia difficile illustrare tendenze e ottenere dati certi sulle vittime, sugli autori e sul loro modus operandi, sia per la mancanza di conoscenze al riguardo che per i rapidi sviluppi (tecnologici) in questo settore. Lo presente studio mostra le caratteristiche principali di questi casi e le cinque categorie di piattaforme che gli autori di reati sessuali online utilizzano più frequentemente.

In Svizzera la protezione dei minori e il perseguimento penale sono principalmente di competenza dei Cantoni. La Confederazione agisce in misura sussidiaria assumendo compiti specifici, per esempio la collaborazione e la cooperazione internazionale con Europol e INTERPOL. Anche le organizzazioni private e le imprese private di telecomunicazione forniscono un contributo importante alla lotta contro i reati in esame. Già oggi dunque il problema viene affrontato ricorrendo a numerose misure giuridiche, tecniche, preventive e di polizia.

Sulla base delle lacune individuate, il gruppo di ricerca ha formulato dieci raccomandazioni per migliorare la protezione di bambini e adolescenti dai reati sessuali online, incentrate sui cinque ambiti seguenti: 1) promozione delle ricerche scientifiche sul tema; 2) rafforzamento del coordinamento e della collaborazione tra gli attori; 3) apertura all'innovazione per le misure preventive; 4) raggiungimento dei gruppi target con un approccio globale; 5) promozione di valutazioni scientifiche per migliorare e consolidare le buone pratiche.

I risultati del presente rapporto di ricerca, integrati nel rapporto del Consiglio federale in adempimento del postulato Quadranti 19.4111, costituiscono una base importante affinché i principali attori coinvolti possano elaborare e/o sviluppare le misure necessarie per garantire una protezione efficace dei minori da abusi sessuali su Internet.

Astrid Wüthrich
Capo dell'Ambito Famiglia, generazioni e società

Foreword by the Federal Social Insurance Office

The postulate submitted by Rosmarie Quadranti [Heinz Siegenthaler] (19.4111) 'Protect children and young people from online predators who seek to incite or coerce them into using their mobile phones to film themselves performing sex acts' calls on the Federal Council to examine the legal, technical and other measures needed to ensure that minors are not induced or blackmailed to produce pornographic material by adults who gain their trust with a view to sexually exploiting them. The Federal Social Insurance Office commissioned the University of Lausanne to investigate the questions posed by the postulate. In addition to looking at legal and technical solutions, the present report explores preventive and police measures, and lays the groundwork for future action.

The study presents the situation in Switzerland, the applicable legislation, and the current state of knowledge about the four types of online sex crimes investigated here: the online production and distribution of child pornography; cybergrooming; sextortion; and the livestreaming of sex acts. The statistics and research to date confirm the prevalence of all four phenomena in Switzerland. Gaps in knowledge and the rapidly changing (technological) developments made it difficult for the research team to map trends and access conclusive data in relation to victims, perpetrators and the modus operandi of the latter. Nonetheless, the study was able to identify the key characteristics of each of these cases, as well as the five types of platforms which perpetrators of online sex crimes use most frequently.

In Switzerland, the cantons are chiefly responsible for child protection and law enforcement. The Confederation acts in a subsidiary capacity and is in charge of specific tasks, such as collaboration and international cooperation with Interpol and Europol. Private organisations and telecommunications companies also play an important role in safeguarding the online safety of minors. The study concludes that a wide range of legal, technical, preventive and police measures have already been taken in Switzerland to tackle the problem.

The research team has formulated ten recommendations to close the gaps in existing knowledge and better protect children and young people from online sex crimes: 1) support for more scientific research; 2) greater coordination and cooperation among actors; 3) a more innovative approach to prevention; 4) reaching target groups through a joined-up approach; and 5) promotion of scientific evaluations to improve and establish good practice.

The Federal Council report on the Quadranti postulate (19.4111) draws on the findings of this study. The results are also an important point of reference for the key actors to devise and/or develop appropriate measures that provide children and young people effective protection from online sex crimes.

Astrid Wüthrich
Head of Families, Generations and Society

Table des matières

Liste des figures

Liste des tableaux

Liste des principales abréviations

AOS	Actes d'ordre sexuel
ASPI	Fondazione Aiuto, Sostegno e Protezione dell'Infanzia
BIK+	The new European strategy for a better internet for kids (Nouvelle stratégie pour un meilleur internet pour les enfants)
CAJ-E	Commission des affaires juridiques du Conseil des Etats
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CCPCS	Conférence des commandantes et des commandants des polices cantonales de Suisse
CCPE	Centre canadien de protection de l'enfance
CP	Code pénal suisse
CPEJ	Conférence pour la politique de l'enfance et de la jeunesse
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DFF	Département fédéral des finances
Ex	Exemple
Fedpol	Office fédéral de la police
Fig	Figure
IA	Intelligence artificielle
ICSE	Internet Child Sexual Exploitation
IRC	Internet Relay Chat (discussion relayée par Internet)
LTC	Loi sur les télécommunications
OFAS	Office fédéral des assurances sociales
OFS	Office fédéral de la statistique
ONG	Organisation non gouvernementale
MPC	Ministère public de la Confédération
NCMEC	National Center for Missing & Exploited Children
NEDIK	Réseau national de soutien aux enquêtes dans la lutte contre la criminalité Informatique
OFROU	Office fédéral des routes
PICSEL	Plateforme d'Informations de la Criminalité Sérielle En Ligne
POLAP	Plateforme d'interrogation de la police
PSC	Prévention Suisse de la Criminalité
RBT	Romandie – Berne – Tessin (concordat de police)
RC3	Centre régional de compétence en cybercriminalité de Genève
SPC	Statistique policière de la criminalité

Tab	Tableau
TIC	Technologies de l'information et de la communication
UNIL	Université de Lausanne
VPN	Virtual Private Network (réseau privé virtuel)

Résumé

CADRE DE L'ÉTUDE

Le 20 décembre 2019, le Conseil national a adopté le postulat 19.4111 Quadranti visant à protéger les enfants incités à se livrer à des actes d'ordre sexuel à l'aide de leur téléphone ou autres appareils permettant une prise de vue photographique ou vidéo. Ce postulat demande au Conseil fédéral d'examiner quelles sont les mesures appropriées pour éviter que les enfants et les jeunes se retrouvent dans des situations dans lesquelles ils seraient incités ou forcés par un adulte à produire du matériel pornographique. En octobre 2021, pour répondre à ce postulat, l'OFAS a mandaté le présent rapport *Mesures de protection des enfants et des jeunes face aux cyber-délits sexuels* à l'Ecole des sciences criminelles de l'Université de Lausanne.

Le mandat se focalise sur quatre comportements en ligne spécifiques :

(a) la **production ou distribution de matériel pédopornographique via Internet**, incluant notamment les représentations de contenus sexuels, focalisées sur les organes sexuels d'un enfant et ayant pour but de susciter une excitation sexuelle ;

(b) le **cyber grooming** – ou pédopiégeage – consistant à entrer en contact avec un enfant sur Internet à des fins sexuelles ;

(c) la **sextorsion** consistant à faire chanter l'enfant suite à l'acquisition de matériel numérique de type sexuel, comme le fait de se procurer des photos osées d'un mineur au travers de réseaux sociaux ;

(d) le **live-streaming d'actes d'ordre sexuel** consistant à diffuser en direct des actes d'ordre sexuel effectués par l'enfant lui-même ou par une personne tierce sur l'enfant.

Le présent rapport est structuré en neuf chapitres. Après l'Introduction (chapitre 1), le contexte suisse est exposé de manière succincte au chapitre 2, en établissant le cadre juridique applicable, l'ampleur des phénomènes enregistrés à travers la statistique policière de la criminalité, ainsi que la répartition des compétences entre les diverses autorités policières et de poursuite pénale. Après avoir illustré la méthodologie utilisée au chapitre 3, les résultats de l'étude sont présentés selon quatre axes au sein du chapitre 4. Le premier introduit, sur la base d'une revue de littérature scientifique, des informations sur les caractéristiques de ces délits ainsi que celles des auteurs et victimes sur la base des études récentes (2016-2021). Le deuxième propose un recensement des acteurs suisses et des réseaux actifs dans la protection des enfants et des jeunes. Le troisième axe décrit une typologie de mesures existantes en Suisse – approches adoptées et groupes cibles –, tout en apportant un éclairage complémentaire en lien avec des initiatives repérées dans d'autres pays. Enfin, le dernier axe relaye l'avis d'experts sur l'évolution des quatre phénomènes étudiés, les réponses qui y sont données, les défis principaux ainsi que les perspectives d'amélioration en matière de protection des enfants et des jeunes. Pour terminer, après une discussion générale sur l'ensemble des résultats (chapitre 5), la conclusion et les recommandations de ce rapport répondent aux questions soulevées dans l'appel d'offre de l'OFAS et proposent des pistes de réflexion pour renforcer la protection des mineurs face aux cyber délits sexuels.

Questions formulées dans l'appel d'offres de l'OFAS

1.1. Où sur Internet et dans quelles situations (types de plateformes et de chats, types d'activités) les différents cyber-délits sexuels ont-ils lieu ? Quelles sont les caractéristiques des victimes et des agresseurs ?

1.2. Quelles mesures existent en Suisse au niveau cantonal, national et international ? Outre les mesures étatiques, les mesures du secteur privé doivent également être incluses (accords d'autorégulation des secteurs, services de plateforme, etc.).

1.3. Qui sont les acteurs et réseaux (par ex. NEDIK) principaux qui proposent des mesures en Suisse ? Quel est leur champ de responsabilité et d'action ?

1.4. À qui s'adressent ces mesures ([potentiels] auteurs du crime, victimes mineures, enfants et jeunes, parents, professionnels, etc.) ?

2.1. Quelles sont les possibilités et les limites de ces mesures ?

2.2. Quelles mesures se montrent particulièrement efficaces ? Peut-on identifier des exemples de bonne pratique en Suisse et à l'étranger ? Dans quelle mesure ces dernières peuvent-elles être applicables en Suisse ?

2.3. Dans quelle mesure existe-t-il des lacunes ?

2.4. Quelles recommandations peuvent être formulées pour la Suisse ?

METHODOLOGIE DE L'ETUDE

Le rapport a mis en œuvre quatre méthodes de récolte de données : 1) une analyse documentaire de la littérature qui a permis d'identifier 105 manuscrits, dont 35 revues de littérature portant sur plusieurs études empiriques, et 70 manuscrits d'études empiriques originales ; 2) un questionnaire structuré en ligne adressé à 447 institutions et à 4 réseaux pour les écoles au sein des 26 cantons suisses sur les acteurs, les initiatives et les collaborations. 134 institutions ont répondu au questionnaire, dont 45 institutions actives dans le domaine de la protection des mineurs contre la cyberdélinquance. En plus, 58 mesures en ligne avec au moins l'un des quatre phénomènes ont été identifiées, ainsi que 22 réseaux / groupes de travail ; 3) une analyse structurée documentaire pour collecter les informations sur les mesures existantes à l'étranger et intégrer les informations sur les mesures suisses. L'analyse a permis d'identifier 188 mesures déployées à travers 29 pays dans le monde (dont 24 en Suisse) ; 4) des entretiens avec des experts pour discuter des phénomènes, des mesures et de leur efficacité en perspective. Dans la période janvier-avril 2022, 18 experts provenant de Suisse ou d'ailleurs ont été interviewés dans le cadre de 15 entretiens (9 femmes et 9 hommes). En croisant toutes les méthodes de collecte de données, l'étude a pu faire état de 257 mesures mises en place dans 29 pays différents, dont 86 en Suisse.

RÉSULTATS

Les cyber-délits sexuels à l'encontre des mineurs

La recherche de littérature a permis de relever certaines caractéristiques principales de ces phénomènes selon les études récentes, notamment en termes de victimes, d'auteurs et de modus operandi en recensant des études menées majoritairement dans des pays anglosaxons. Au niveau de la Suisse, un manque de données est relevé. Par ailleurs, les indicateurs pour observer les phénomènes de cyberdélinquance sexuelle (statistiques de la criminalité, sondage de victimisation, autres enquêtes publiques et privées) sont récents et, dans l'état actuel, ils ne permettent pas de fournir des interprétations ni sur l'ampleur ni sur les tendances de la criminalité.

Les entretiens avec les experts ont permis toutefois d'identifier certains points d'attention observés dans leur pratique quant à l'évolution de ces délits, les plateformes utilisées, ainsi que les caractéristiques des victimes/auteurs.

Globalement, les experts interviewés constatent ou présument que les cyber-délits sexuels à l'encontre de mineurs sont en augmentation. Toutefois, cette tendance n'est pas toujours visible dans les statistiques, laissant penser que l'augmentation est à considérer dans le chiffre noir de la criminalité.

Les plateformes fréquentées par les jeunes sont des espaces attractifs pour les auteurs de cyber-délits sexuels envers les mineurs afin d'entrer en contact avec ces derniers. Ces plateformes sont parfois utilisées uniquement comme point d'accroche pour ensuite se déplacer vers une messagerie cryptée. Toutefois, il n'est pas possible d'établir une liste exhaustive des plateformes, celles-ci variant au gré de la mode et des avancées technologiques. En revanche, des types de plateformes ont été identifiés, comme les réseaux sociaux, les jeux vidéo en ligne, les sites réservés aux adultes (ex. sites érotiques), les messageries instantanées et le Dark web.

En ce qui concerne les caractéristiques des victimes et des agresseurs, il n'y a pas de profil type au sens strict. Les affaires de cyber-délits sexuels indiquent que les victimes et les auteurs proviennent de toutes classes d'âge, de toutes classes sociales, etc. En l'état actuel, les statistiques policières sur la criminalité sexuelle présentent une majorité de victimes mineures de sexe féminin et une prédominance de personnes prévenues d'âge adulte et de sexe masculin. Néanmoins, il convient de souligner que les scientifiques ont remarqué un certain nombre de problèmes de représentativité des données policières – celles-ci apportant qu'une vision partielle de la criminalité réelle – surtout dans le domaine de la délinquance sexuelle. En ce sens, il est délicat de mettre en évidence des caractéristiques, car les informations peuvent être généralisées et mal interprétées, surtout pour des phénomènes plus récents (ex. live-streaming) où les connaissances académiques et des experts, de même que les dénonciations aux autorités policières restent anecdotiques.

Les acteurs investis dans la protection des mineurs en ligne

De manière générale, une pluralité d'acteurs s'est saisie de cette thématique, que ce soit au niveau étatique (départements et offices de gouvernement, corps de police), associatif, de l'industrie (notamment les entreprises privées de télécommunication), ou encore du milieu scolaire public ou privé.

Ces acteurs s'occupent de traiter les questions liées aux cyber-délits sexuels en fonction de leur champ de responsabilité ou leur domaine d'expertise. Alors que le milieu scolaire contribue principalement à enseigner une bonne hygiène numérique, les associations et fondations fournissent surtout des conseils et développent des plateformes d'aide et des activités ludiques. En tant que fournisseurs de services de télécommunication, certaines entreprises privées sont impliquées dans la protection des enfants et des jeunes en proposant avant tout des mesures techniques, mais certaines conçoivent aussi des cours de sensibilisation ou financent des études sur l'utilisation des médias. Les départements et offices du gouvernement développent des collaborations avec d'autres institutions ou partenaires, et des mesures de sensibilisation pour le grand public. Enfin, la police combine un travail répressif en poursuivant la détection et l'investigation des cyber-délits sexuels et un travail de prévention avec des échanges d'informations, des cours de sensibilisation et une présence en ligne tant préventive que répressive.

Les mesures recensées en Suisse

La présente étude constate le développement d'une pluralité de mesures en Suisse. Sur 86 mesures identifiées, plus de la moitié sont implémentées ou rendues accessibles à une échelle cantonale, voire locale. Les initiatives développées dans une perspective nationale représentent un peu plus d'un quart des mesures identifiées. Enfin, d'autres mesures trouvent une portée plus régionale.

Les mesures recensées sont regroupées en quatre catégories : préventives, techniques, policières et juridiques. Dans les *mesures préventives,* la majorité des mesures prennent la forme de formation (cours de sensibilisation) ou de mise à disposition d'informations et de conseils (sur des sites Internet, en format brochures, etc.). Des activités ludiques, des mesures d'aide et soutien (sans option de traitement), ainsi qu'une campagne de sensibilisation à l'échelle nationale, ont également été recensées. En ce qui concerne les *mesures techniques*, des logiciels/applications de contrôle et de blocage proposés par des services de télécommunication ou associations sont relevés. En outre, des plateformes de signalements sont mises à disposition de la population afin de signaler une cyber infraction ou la découverte d'un matériel de pornographie interdite – y compris la pornographie enfantine – sur Internet. Enfin, certaines écoles adoptent des chartes de sécurité rappelant les règles de bonne conduite aux élèves. Quant aux *mesures policières*, certains moyens d'investigation ne peuvent pas être publiquement divulgués afin d'assurer la bonne continuité du travail des forces de l'ordre. Sans entrer dans les détails opérationnels, nous mentionnons que le suivi des annonces du National Center for Missing & Exploited Children (NCMEC), le blocage de site Internet, les recherches secrètes préventives, les bases de données de police nationales et internationales, les collaborations avec d'autres autorités policières/judiciaires étrangères font partis des outils et méthodes policières contribuant à la prévention et à la lutte contre la délinquance sexuelle en ligne à l'encontre des mineurs. Enfin, les *mesures juridiques* font référence au droit pénal suisse en vigueur qui criminalise les quatre phénomènes étudiés dans ce mandat.

Le public cible des mesures recensées en Suisse

Presque la moitié des mesures sont destinées aux enfants et aux jeunes, suivent les mesures adressées aux parents. Peu d'initiatives semblent formulées pour les enseignants et autres professionnels travaillant avec des enfants et des adolescents. Or, la capacité d'action de la prévention se trouve

limitée dès lors qu'elle n'inclut pas l'environnement des enfants et des jeunes, à savoir les enseignants et la communauté au sens large. De plus, les mesures qui tendent à modifier l'environnement – situations –sont plus rares.

D'autre part, la plupart des mesures de prévention relevées en Suisse sont conçues pour les (potentielles) victimes. De ce fait, la prévention devrait également s'adresser aux (potentiels) auteurs en vue d'empêcher le passage à l'acte ou la récidive.

Limitations, lacunes et pistes de réflexion

Cinq points d'attention ont été mis en exergue dans le cadre de cette étude.

- *Connaissances lacunaires* : un manque de données concernant le cyber grooming, la sextorsion et le live-streaming est relevé, notamment en ce qui concerne les études académiques. En effet, les études recensées sur les quatre phénomènes d'intérêt proviennent majoritairement des pays anglosaxons. Ainsi, un renforcement des recherches, également en Suisse, permettraient de mieux connaitre ces phénomènes et de concevoir des mesures de prévention en adéquation avec leur évolution.
- *Complexité dans la coordination des acteurs* : de manière générale, une pluralité d'acteurs s'est saisie de cette thématique, que ce soit au niveau étatique, associatif, de l'industrie ou encore du milieu scolaire. Néanmoins, une approche en silo est davantage relevée qu'une approche transversale. Mise à part dans le domaine policier où la coopération internationale s'est fortement développée pour lutter contre l'exploitation sexuelle des mineurs sur Internet, des marges d'amélioration subsistent dans les collaborations intra et inter domaine d'activité. Il serait ainsi bénéfique de renforcer les réseaux existants ainsi que des partenariats public-privé qui pourraient agir comme facteur d'harmonisation et de systématisation des connaissances et des compétences.
- *Mesures dissociées et plutôt traditionnelles* : l'implémentation de mesures dissociées est observée, dû notamment au fait que les acteurs ne s'organisent pas toujours en réseaux. D'autre part, la majorité des mesures identifiées en Suisse prennent la forme de formation (sensibilisation) ou de mise à disposition d'informations et de conseils (sur des sites Internet, brochures, etc.) qui sont des mesures relativement classiques. La prévention pourrait dès lors tendre vers des initiatives plus diversifiées alliant divertissement et messages éducatifs, tout en accroissant la présence sur les canaux de communication populaires auprès des groupes cibles (par ex. pour les jeunes, les réseaux sociaux et les plateformes de jeux vidéo).
- *Approche orientée principalement vers les jeunes et les (potentielles) victimes* : la majorité des initiatives de prévention s'adressent principalement aux enfants et aux jeunes, considérés comme un groupe vulnérable et des victimes potentielles. Or, la capacité d'action de la prévention se trouve limitée dès lors qu'elle n'inclut pas l'ensemble de l'environnement des enfants. En ce sens, une approche holistique est à privilégier. Par ailleurs, la prévention devrait également s'adresser aux (potentiels) auteurs en vue d'empêcher le passage à l'acte ou la récidive. Dans cette perspective de prévention secondaire et tertiaire, le système de soutien et d'aide (avec et sans option de traitement) aux personnes ayant une attirance sexuelle pour les

mineurs ou ayant commis un délit sexuel en ligne à l'encontre des mineurs pourrait être renforcé.

- *Difficulté à identifier les bonnes pratiques dans le milieu de la détection et de la prévention* : La dispersion des informations peut également représenter un obstacle dans la compréhension et dans les solutions à proposer pour prévenir et lutter contre les cyber-délits sexuels. Le développement d'outils de renseignements, de suivi et de détection de situation permettrait d'améliorer la vision de ces phénomènes et d'optimiser les prises de décisions stratégiques et opérationnelles. D'autre part, il ressort de l'étude qu'il est difficile d'établir, d'un point de vue scientifique, quelles sont les mesures les plus efficaces. En effet, les évaluations sur les programmes de prévention en la matière – en Suisse et ailleurs – sont très pauvres. De ce fait, la mise en œuvre de processus d'évaluation d'efficacité des programmes de prévention devrait être encouragée et soutenue afin de les perfectionner si nécessaire et de créer du savoir issu des pratiques.

RECOMMANDATIONS

Sur la base des informations recensées dans ce rapport, dix recommandations ont été formulées en vue de travailler sur les perspectives d'évolution susmentionnées et d'améliorer la capacité du système suisse à répondre à ces phénomènes de cyber-délits sexuels à l'encontre des mineurs.

1. Encourager et soutenir les recherches scientifiques sur la thématique des cyber-délits sexuels à l'encontre des mineurs.
2. Développer une stratégie nationale pour la prévention des cyber-délits sexuels envers les mineurs.
3. Renforcer les partenariats public-privé pour le monitoring, le triage et le partage de données.
4. Soutenir l'harmonisation des bases légales pour permettre l'échange de données lors des enquêtes.
5. Développer des mesures en alliant divertissement et messages éducatifs, tout en accroissant la présence sur les canaux de communication populaires auprès des groupes cibles (par ex. pour les jeunes, les réseaux sociaux et les plateformes de jeux vidéo).
6. Octroyer un rôle actif aux mineurs dans la conception et l'application des mesures de prévention.
7. Renforcer la formation des enseignants et des professionnels du milieu de la jeunesse. Des connaissances plus pointues sur ces phénomènes leur permettraient de mieux encadrer et soutenir les enfants et les jeunes.
8. Soutenir le développement et la promotion d'un réseau de soutien et d'aide (avec et sans option de traitement) pour les victimes et les (potentiels) auteurs.
9. Développer des outils de renseignements, de suivi et de détection de situation.
10. Encourager et soutenir l'évaluation scientifique de programmes de prévention.

Zusammenfassung

KONTEXT

Am 20. Dezember 2019 hat der Bundesrat das Postulat 19.4111 Quadranti angenommen, das Kinder und Jugendliche davor schützen will, zu sexuellen Handlungen gedrängt zu werden und sich dabei mit ihrem Handy oder anderen Geräten zu fotografieren oder zu filmen. Das Postulat verlangt vom Bundesrat, geeignete Massnahmen zu prüfen, damit Kinder und Jugendliche nicht in eine Situation geraten, in der sie von Erwachsenen zur Herstellung von kinderpornografischem Material erpresst oder angeleitet werden. Zur Erfüllung des Postulats hat das BSV im Oktober 2021 bei der *Ecole des sciences criminelles* der Universität Lausanne den Bericht *Mesures de protection des enfants et des jeunes face aux cyber-délits sexuels* in Auftrag gegeben.

Die Studie konzentriert sich auf vier spezifische Verhaltensweisen im Internet:

(a) die **Herstellung oder Verbreitung von pädopornografischem Material**, insbesondere die Darstellung von sexuellen Inhalten, die auf die Geschlechtsteile eines Kindes fokussiert und sexuelle Erregung hervorrufen soll;

(b) **Cybergrooming** als Anbahnung sexueller Kontakte mit Kindern im Internet;

(c) **Sextortion**, wobei das Kind mit digitalen sexuellen Inhalten erpresst wird, beispielsweise wenn über soziale Netzwerke freizügige Bilder einer minderjährigen Person beschafft werden;

(d) **Live-Streaming sexueller Handlungen**, wobei sexuelle Handlungen vom Kind selbst oder von einer Drittperson beim Kind durchgeführt und live übertragen werden.

Der vorliegende Bericht ist in neun Kapitel gegliedert. Nach der Einleitung (Kap. 1) geht Kapitel 2 kurz auf den Schweizer Kontext ein. Dabei wird der geltende Rechtsrahmen, das Ausmass der in der polizeilichen Kriminalstatistik erfassten Straftaten und die Kompetenzaufteilung zwischen den verschiedenen Polizei- und Strafverfolgungsbehörden erläutert. Kapitel 3 beschreibt die angewandte Methodik. Kapitel 4 erörtert die Ergebnisse der Studie anhand von vier Schwerpunkten: Einleitend werden gestützt auf eine Analyse der neueren Fachliteratur (Studien von 2016–2021) die Merkmale der Delikte sowie der Täterschaft und der Opfer erläutert. Im zweiten Schwerpunkt werden die in der Schweiz tätigen Akteure sowie die im Kinder- und Jugendschutz aktiven Netzwerke vorgestellt. Es folgt eine Typologie der bestehenden Massnahmen in der Schweiz nach Ansätzen und Zielgruppen, wobei ergänzend auf Initiativen in anderen Ländern Bezug genommen wird. Der vierte Schwerpunkt beleuchtet die Sichtweise von Expertinnen und Experten auf die Entwicklung der vier untersuchten Tatbestände, den Umgang damit sowie die Herausforderungen und Verbesserungsmöglichkeiten im Bereich des Kinder- und Jugendschutzes. Nach einer allgemeinen Diskussion der Ergebnisse (Kap. 5) behandelt der Bericht anhand von Schlussfolgerungen und Empfehlungen die *Forschungsfrage*n des BSV und liefert Denkanstösse zur Stärkung des Schutzes von Minderjährigen vor Cyber-Sexualdelikten.

Fragestellung des BSV-Forschungsauftrags

1.1. Wo im Internet und in welchen Situationen (Arten von Plattformen und Chaträumen, Arten von Tätigkeiten) finden die verschiedenen Cyber-Sexualdelikte statt? Welche Charakteristiken/Merkmale weisen die Opfer und die Täter auf?

1.2. Welche Massnahmen gibt es in der Schweiz auf kantonaler, nationaler und internationaler Ebene? Neben staatlichen Massnahmen sollen auch diejenigen aus der Privatwirtschaft (Selbstregulierungs-Vereinbarungen der Branchen, Plattformdiensten etc.) einbezogen werden.

1.3. Wer sind die wichtigsten Akteurinnen/Akteure und Netzwerke (z. B. NEDIK) dieser Massnahmen in der Schweiz? Was ist ihr Verantwortungs- und Wirkungsbereich?

1.4. An wen richten sich die Massnahmen ([potenzielle] Straftäter, minderjährige Opfer, Kinder und Jugendliche, Eltern, Fachpersonen usw.)?

2.1. Was sind die Möglichkeiten und die Grenzen dieser Massnahmen?

2.2. Welche Massnahmen erweisen sich als besonders erfolgsversprechend? Können Beispiele guter Praxis in der Schweiz und im Ausland identifiziert werden? Inwiefern sind Letztere auf die Schweiz übertragbar?

2.3. Inwiefern bestehen Lücken?

2.4. Welche Empfehlungen lassen sich für die Schweiz formulieren?

METHODIK DER STUDIE

Die Studie greift auf vier Methoden der Datenerhebung zurück: 1) eine Analyse der Fachliteratur anhand von 105 Studien, darunter 35 Metastudien zu mehreren empirischen Studien; 2) ein strukturierter Online-Fragebogen zu den Akteuren, Initiativen und der Zusammenarbeit, der an 447 Institutionen und 4 Netzwerke für die Schulen in den 26 Kantonen gesendet wurde. 134 Institutionen füllten den Fragebogen aus, darunter 45 Institutionen, die im Bereich des Schutzes von Minderjährigen vor Cyberkriminalität tätig sind. Zudem wurden 58 Massnahmen mit Bezug zu mindestens einem der vier Tatbestände sowie 22 Netzwerke/Arbeitsgruppen identifiziert; 3) eine strukturierte Dokumentenanalyse zur Informationsgewinnung über bestehende Massnahmen im Ausland und in der Schweiz. Hier wurden 188 Massnahmen in weltweit 29 Ländern ermittelt (darunter 24 aus der Schweiz); 4) Interviews mit Expertinnen und Experten, um die Tatbestände, die Massnahmen und deren erwartete Wirksamkeit zu erörtern. Zwischen Januar und April 2022 wurden im Rahmen von 15 Gesprächen 18 schweizerische und ausländische Expertinnen und Experten (9 Frauen und 9 Männer) befragt. Alle Methoden der Datenerhebung zusammengenommen, identifiziert die Studie insgesamt 257 Massnahmen in 29 Ländern, davon 86 in der Schweiz.

ERGEBNISSE

Cyber-Sexualdelikte gegen Minderjährige

Anhand der Literaturrecherche konnten einige wichtige Merkmale der Tatbestände gemäss neusten Studien ausgemacht werden, insbesondere in Bezug auf die Opfer, die Täterschaft und das Tatvorgehen. Die erfassten Studien stammen mehrheitlich aus dem angelsächsischen Raum. Für die Schweiz fehlt es an Daten zum Thema. Zudem sind die Indikatoren zur Beobachtung der Cyber-Sexualdelikte (Kriminalstatistiken, Umfragen zur Viktimisierung, andere öffentliche und private Erhebungen) noch sehr neu und erlauben zum jetzigen Zeitpunkt keine Aussagen zu Ausmass oder Trends der Kriminalität in diesem Bereich.

Aus den Experteninterviews lassen sich jedoch gewisse Schlüsse aus der Praxis in Bezug auf die Entwicklung der Delikte, die verwendeten Plattformen und die Merkmale der Opfer bzw. der Täterschaft ziehen.

Insgesamt konstatieren oder vermuten die befragten Expertinnen und Experten, dass die Cyber-Sexualdelikte gegen Minderjährige zunehmen. Diese Entwicklung wird jedoch in den Statistiken nicht immer sichtbar, was darauf schliessen lässt, dass die Zunahme in der Dunkelziffer dieser Form von Kriminalität zu suchen ist.

Von den Jugendlichen besuchte Plattformen sind für Täter von Cyber-Sexualdelikten gegen Minderjährige attraktive Räume, um mit ihren Opfern Kontakt aufzunehmen. Manchmal dienen die Plattformen nur als Ausgangspunkt, bevor die Konversation auf einem verschlüsselten Nachrichtendienst weitergeführt wird. Eine abschliessende Auflistung solcher Plattformen ist aufgrund von wechselnden Trends und neuen technischen Entwicklungen nicht möglich. Dennoch können Plattformtypen identifiziert werden, namentlich soziale Netzwerke, Online-Games, Webseiten, die ausschliesslich für Erwachsene bestimmt sind (z. B. Erotik-Seiten), Instant-Messaging-Dienste und das Dark Web.

In Bezug auf die Eigenschaften der Opfer sowie der Täter lässt sich kein typisches Profil im engeren Sinne definieren. Fälle von Cyber-Sexualdelikten zeigen, dass Opfer und Täter aus allen Altersklassen, sozialen Schichten usw. stammen. Aktuell weisen die polizeilichen Statistiken zur Sexualkriminalität unter den Opfern eine Mehrheit an minderjährigen weiblichen Betroffenen und unter den Beschuldigten eine Mehrheit männlicher Erwachsener aus. Wissenschaftlerinnen und Wissenschaftler weisen jedoch auf gewisse Probleme in Bezug auf die Repräsentativität der Polizeidaten hin und unterstreichen, dass die tatsächliche Kriminalität nur unvollständig abgebildet werde, vor allem im Bereich der Sexualdelinquenz. Deshalb ist es heikel, spezifische Merkmale hervorzuheben, da solche Angaben pauschalisiert und falsch interpretiert werden könnten. Dies gilt insbesondere für neuere Formen (z. B. Live-Streaming), zu denen nur sehr spärliche Forschungs- und Expertendaten sowie polizeiliche Verzeigungen vorliegen.

Schutz Minderjähriger vor Internetrisiken: Akteure

Zahlreiche Akteure befassen sich mit dem Schutz Minderjähriger vor Internetrisiken. Dazu zählen namentlich staatliche Stellen (Departemente und Ämter des Bundes, Polizeikorps), Vereine,

Unternehmen (insbesondere private Telekommunikationsunternehmen) sowie öffentliche und private Schulen.

In ihrem Verantwortungs- und Kompetenzbereich greifen sie gezielt Fragen im Zusammenhang mit Cyber-Sexualdelikten auf. Während die Schulen vor allem dazu beitragen, eine gute «digitale Hygiene» zu vermitteln, bieten Vereine und Stiftungen hauptsächlich Beratung und entwickeln Unterstützungsplattformen sowie spielerische Aktivitäten. Auch Telekommunikationsunternehmen sind in den Kinder- und Jugendschutz eingebunden, wobei manche Privatunternehmen insbesondere technische Massnahmen bereitstellen, während andere auch Sensibilisierungskurse erarbeiten oder Studien zur Mediennutzung finanzieren. Die Departemente und Ämter des Bundes entwickeln Formen der Zusammenarbeit mit anderen Institutionen oder Partnern sowie Sensibilisierungsangebote für die breite Öffentlichkeit. Die Polizei schliesslich kombiniert repressives Vorgehen im Bereich Aufdeckung und Untersuchung von Cyber-Sexualdelikten mit präventiven Tätigkeiten wie Informationsaustausch oder Sensibilisierungskursen. Zudem ist sie sowohl zu präventiven als auch repressiven Zwecken auf dem Internet präsent.

In der Schweiz erhobene Massnahmen

Die vorliegende Studie stellt fest, dass in der Schweiz eine Vielfalt von Massnahmen entwickelt wurden. Mehr als die Hälfte der 86 erfassten Massnahmen werden auf kantonaler oder lokaler Ebene umgesetzt, beziehungsweise zugänglich gemacht. Etwas mehr als ein Viertel der Initiativen sind national ausgerichtet, die übrigen haben eine regionale Reichweite.

Die erhobenen Massnahmen umfassen vier Kategorien: präventive, technische, polizeiliche und rechtliche Massnahmen. Bei den *präventiven Massnahmen* geht es meistens um Lernaspekte (Sensibilisierungskurse) oder die Bereitstellung von Informationen und Beratung (auf Internetseiten, in Broschüren usw.). Ebenfalls erfasst wurden spielerische Aktivitäten, Hilfs- und Unterstützungsmassnahmen (ohne Behandlungsmöglichkeit) sowie eine Sensibilisierungskampagne auf nationaler Ebene. Zu den *technischen Massnahmen* zählen Kontroll- und Sperrsoftware bzw. -anwendungen, wie sie von Telekommunikationsunternehmen oder Vereinen angeboten werden. Ausserdem stehen der Bevölkerung Meldeplattformen zur Verfügung, über die eine Cyberstraftat oder verbotenes pornografisches Material – einschliesslich Kinderpornografie – auf dem Internet gemeldet werden kann. Einige Schulen haben überdies Sicherheitschartas verabschiedet, die den Schülerinnen und Schülern Verhaltensregeln aufzeigen. Im Bereich der *polizeilichen Massnahmen* dürfen gewisse Ermittlungsmethoden nicht öffentlich gemacht werden, um die Arbeit der Sicherheitskräfte nicht zu gefährden. Ohne auf operative Details einzugehen, können indessen die ständige Überprüfung der Meldungen des *National Center for Missing & Exploited Children* (NCMEC), die Sperrung von Internetseiten, geheime präventive Recherchen, nationale und internationale Polizeidatenbanken oder die Zusammenarbeit mit anderen ausländischen Polizei- und Justizbehörden als Instrumente und Methoden der Polizei erwähnt werden, die zur Prävention und Bekämpfung von Sexualdelikten gegen Minderjährige über das Internet beitragen. Die *rechtlichen Massnahmen* schliesslich betreffen das schweizerische Strafrecht, das die vier mit diesem Forschungsauftrag untersuchten Tatbestände unter Strafe stellt.

Zielpublikum der Massnahmen in der Schweiz

Fast die Hälfte der Massnahmen richtet sich an Kinder und Jugendliche. An zweiter Stelle stehen elternspezifische Massnahmen. Nur wenige Initiativen zielen spezifisch auf Lehrkräfte oder andere Berufsgruppen, die mit Kindern und Jugendlichen arbeiten. Der Wirkungsbereich der Prävention ist damit insofern eingeschränkt, als das Umfeld der Kinder und Jugendlichen – Lehrpersonen und die Gemeinschaft im weiteren Sinne – nicht einbezogen wird. Auch Massnahmen, die auf eine Veränderung des Umfelds (der Situationen) abzielen, gibt es kaum.

Darüber hinaus sind die meisten in der Schweiz erhobenen präventiven Massnahmen auf (potenzielle) Opfer ausgerichtet. Deshalb sollte sich die Prävention auch um (potenzielle) Täter kümmern, um das Begehen der Tat oder Rückfälle zu verhindern.

Grenzen, Lücken und Denkanstösse

Im Rahmen der Studie wurden fünf Fokuspunkte hervorgehoben:

- *Lückenhafte Kenntnisse:* Es fehlt an Daten und insbesondere wissenschaftlichen Studien zu Cybergrooming, Sextortion und Live-Streaming. Die vorhandenen Studien zu den vier betrachteten Tatbeständen stammen mehrheitlich aus dem angelsächsischen Raum. Mehr Untersuchungen, auch in der Schweiz, könnten das Wissen über Cyber-Sexualstraftaten verbessern und dazu beitragen, ihrer Entwicklung entsprechende Präventionsmassnahmen zu erarbeiten.
- *Komplexe Koordination der Akteure:* Insgesamt befassen sich zahlreiche Akteure auf Staats-, Vereins-, Unternehmens- und Schulebene mit diesem Thema. Dabei agieren sie jedoch eher isoliert als übergreifend. Abgesehen vom polizeilichen Bereich, in dem die internationale Kooperation zur Bekämpfung der sexuellen Ausbeutung von Minderjährigen über das Internet stark ausgebaut wurde, besteht bei der Zusammenarbeit innerhalb und zwischen den Tätigkeitsbereichen noch Verbesserungspotenzial. Deshalb wäre es sinnvoll, die bestehenden Netzwerke und öffentlich-privaten Partnerschaften zu verstärken, um die Harmonisierung und die Systematisierung der Kenntnisse und Kompetenzen voranzutreiben.
- *Unkoordinierte und eher traditionelle Massnahmen:* Es zeigt sich einerseits, dass Massnahmen oft unkoordiniert eingeführt werden, hauptsächlich weil die Akteure nicht immer vernetzt sind. Andererseits handelt es sich bei den meisten in der Schweiz erfassten Massnahmen um Lernformate (Sensibilisierung) oder Informations- und Beratungsangebote (Internetseiten, Broschüren usw.), also um relativ klassische Massnahmen. In der Prävention könnte man deshalb auf eine Diversifizierung der Initiativen hinwirken, beispielsweise durch eine Verbindung des Unterhaltungsaspekts und pädagogischen Botschaften. Zudem könnte die Präsenz auf den bei den Zielgruppen beliebten Kommunikationskanälen ausgebaut werden (für die Jugendlichen z. B. auf sozialen Netzwerken und Gaming-Plattformen).
- *Hauptsächlich auf Jugendliche und (potenzielle) Opfer ausgerichteter Ansatz:* Die Mehrheit der Präventionsinitiativen richtet sich primär an Kinder und Jugendliche als gefährdete Gruppe und potenzielle Opfer. Damit wird das Wirkungspotenzial der Prävention jedoch eingeschränkt, da nicht das gesamte Umfeld der Kinder erfasst wird. Deshalb sollte ein

ganzheitlicher Ansatz angestrebt werden. Die Prävention müsste sich ausserdem auch an (potenzielle) Täter richten, um das Begehen der Tat oder Rückfälle zu verhindern. Unter diesem Gesichtspunkt der sekundären und tertiären Prävention könnte das Unterstützungs- und Beratungssystem (mit oder ohne Behandlungsmöglichkeit) für Personen mit einem sexuellen Interesse an Kindern oder für bereits straffällig gewordene Personen verstärkt werden.

- *Erschwerte Identifikation von Good Pratice im Bereich Erkennung und Prävention:* Verstreute Informationen können das Verständnis und die Suche nach Lösungen zur Prävention und zur Bekämpfung von Cyber-Sexualdelikten erschweren. Die Entwicklung von Auskunfts-, Überwachungs- und Erkennungsinstrumenten könnte die Sichtbarkeit entsprechender Vorkommnisse und die strategischen und operativen Entscheidungsfindungsprozesse verbessern. Gleichzeitig zeigt die Studie auch, dass es schwierig ist, wissenschaftlich zu beurteilen, welche Massnahmen am wirkungsvollsten sind. Evaluationen zu den Präventionsprogrammen sind sowohl in der Schweiz als auch im Ausland wenig aussagekräftig. Aus diesem Grund sollten Evaluationen der Wirksamkeit von Präventionsprogrammen gefördert und unterstützt werden, damit diese, wenn nötig, optimiert und Erkenntnisse daraus gezogen werden können.

EMPFEHLUNGEN

Anhand der erhobenen Informationen können zehn Empfehlungen formuliert werden, wie auf die oben beschriebenen Entwicklungsperspektiven hingearbeitet werden kann und wie sich das Schweizer System zur Bekämpfung von Cyber-Sexualdelikten gegen Minderjährige insgesamt verbessern lässt.

11. Wissenschaftliche Forschung zum Thema Cyber-Sexualdelikte gegen Minderjährige fördern und unterstützen.
12. Eine nationale Strategie zur Prävention von Cyber-Sexualdelikten gegen Minderjährige entwickeln.
13. Öffentlich-private Partnerschaften für das Monitoring, die Triage und den Datenaustausch stärken.
14. Die Harmonisierung der Gesetzesgrundlagen unterstützen, um den Datenaustausch im Rahmen von Ermittlungen zu erleichtern.
15. Massnahmen erarbeiten, die den Unterhaltungsaspekt und pädagogische Botschaften verbinden und dabei die Präsenz auf den bei den Zielgruppen beliebten Kommunikationskanälen ausbauen (für die Jugendlichen z. B. auf sozialen Netzwerken und Gaming-Plattformen).
16. Den Jugendlichen bei der Entwicklung und Anwendung der Präventionsmassnahmen eine aktive Rolle zuweisen.
17. Die Ausbildung der Lehrkräfte und der Fachpersonen im Jugendbereich verstärken. Fundiertere Kenntnisse zu den entsprechenden Tatbeständen könnten ihnen bei der Begleitung und Unterstützung der Kinder und Jugendlichen helfen.

18. Die Schaffung und Förderung eines Unterstützungs- und Beratungsnetzwerks (mit oder ohne Behandlungsmöglichkeit) für Opfer und (potenzielle) Täter unterstützen.
19. Auskunfts-, Überwachungs- und Erkennungsinstrumente entwickeln.
20. Die wissenschaftliche Evaluation von Präventionsprogrammen fördern und unterstützen.

Riassunto

CONTESTO DELLO STUDIO

Il 20 dicembre 2019 il Consiglio nazionale ha accolto il postulato 19.4111 Quadranti, teso a proteggere i minori indotti a compiere atti sessuali davanti a cellulari o altri apparecchi che permettono di registrare video o scattare fotografie. Questo postulato chiede al Consiglio federale di esaminare quali siano le misure appropriate per evitare che bambini e adolescenti si ritrovino in situazioni in cui vengono indotti o forzati da un adulto a produrre materiale pornografico. Nell'ottobre del 2021, per adempiere il postulato, l'Ufficio federale delle assicurazioni sociali (UFAS) ha commissionato il presente rapporto alla Scuola di criminologia dell'Università di Losanna.

Il mandato si concentra su quattro comportamenti online specifici:

(a) la **produzione o distribuzione di materiale pedopornografico tramite Internet**, che include in particolare le rappresentazioni di contenuti sessuali incentrati sugli organi sessuali di un minore e tese a suscitare eccitazione sessuale;

(b) il **cibergrooming** (o adescamento di minori), che consiste nel contattare un minore su Internet a fini sessuali;

(c) la **sextortion**, che consiste nel ricattare un minore dopo aver acquisito materiale digitale a sfondo sessuale, ad esempio per procurarsi sue foto spinte attraverso le reti sociali;

(d) il **live streaming di atti sessuali**, che consiste nel diffondere in diretta atti sessuali compiuti direttamente da un minore o da una terza persona sul minore.

Il presente rapporto è strutturato in nove capitoli. Dopo l'introduzione (capitolo 1), nel capitolo 2 è sinteticamente esposto il contesto svizzero per stabilire il quadro giuridico applicabile, l'ampiezza dei fenomeni registrati mediante la statistica criminale di polizia nonché la ripartizione delle competenze tra le diverse autorità di polizia e di perseguimento penale. Dopo aver illustrato nel capitolo 3 la metodologia utilizzata, i risultati dello studio sono presentati nel capitolo 4 secondo quattro assi. Il primo introduce, fondandosi su una rassegna della letteratura scientifica, informazioni sulle caratteristiche dei reati in questione nonché degli autori e delle vittime sulla base di studi recenti (2016–2021). Il secondo propone una rilevazione degli attori svizzeri e delle reti attive nella protezione dei bambini e degli adolescenti. Il terzo descrive una tipologia di misure esistenti in Svizzera (approcci adottati e gruppi target), aggiungendo una chiarificazione complementare in merito alle iniziative applicate in altri Paesi. L'ultimo asse riporta il parere di esperti sull'evoluzione dei quattro fenomeni oggetto dello studio, le risposte che vi vengono date, le sfide principali e le prospettive di miglioramento nel contesto della protezione di bambini e adolescenti. Per finire, dopo una discussione generale sull'insieme dei risultati (capitolo 5), la conclusione e le raccomandazioni di questo rapporto rispondono agli interrogativi sollevati nel bando di concorso dell'UFAS e propongono spunti di riflessione per rafforzare la protezione dei minori dai reati sessuali online.

Questioni formulate nel bando di concorso dell'UFAS

1.1. Dove su Internet e in quali situazioni (tipo di piattaforma e di chat, tipo di attività) vengono commessi i differenti reati sessuali online? Quali sono le caratteristiche delle vittime e degli autori?

1.2. Quali misure esistono in Svizzera, stabilite a livello cantonale, nazionale e internazionale? Oltre alle misure statali devono essere incluse anche le misure del settore privato (accordi settoriali di autoregolamentazione, servizi di piattaforma ecc.).

1.3. Quali sono gli attori e le reti (p. es. NEDIK) principali che propongono misure in Svizzera? Quali sono il loro settore di responsabilità e il loro campo d'azione?

1.4. A chi sono rivolte queste misure ([potenziali] attori dei reati, vittime minorenni, bambini e adolescenti, genitori, operatori dei settori interessati ecc.)?

2.1. Quali sono le potenzialità e i limiti di queste misure?

2.2. Quali misure si rivelano particolarmente efficaci? È possibile identificare esempi di buone pratiche in Svizzera e all'estero? In che misura queste ultime possono essere attuate in Svizzera?

2.3. In che misura esistono lacune?

2.4. Quali raccomandazioni possono essere formulate per la Svizzera?

METODOLOGIA DELLO STUDIO

Nel quadro del rapporto sono stati adottati quattro metodi per la raccolta dei dati: 1) un'analisi documentale della letteratura scientifica che ha permesso di identificare 105 manoscritti, di cui 35 riviste di letteratura relative a numerosi studi empirici e 70 manoscritti di studi empirici originali; 2) un questionario strutturato online indirizzato a 447 istituzioni e a 4 reti per le scuole distribuiti nei 26 Cantoni svizzeri su attori, iniziative e collaborazioni. Al questionario hanno risposto 134 istituzioni, di cui 45 attive nell'ambito della protezione dei minori contro la cibercriminalità. Inoltre, sono state identificate 58 misure online con almeno uno dei quattro fenomeni trattati nonché 22 reti/gruppi di lavoro; 3) un'analisi strutturata documentale per raccogliere le informazioni sulle misure esistenti all'estero e integrare informazioni sulle misure svizzere. L'analisi ha permesso di identificare 188 misure attuate in 29 Paesi del mondo (di cui 24 in Svizzera); 4) colloqui con esperti per discutere i fenomeni, le misure e la loro efficacia in prospettiva. Nel periodo gennaio–aprile 2022, 18 esperti (9 donne e 9 uomini) provenienti dalla Svizzera e dall'estero sono stati intervistati nel quadro di 15 colloqui. Incrociando tutti i metodi di raccolta di dati, nello studio è stato possibile rilevare 257 misure attuate in 29 Paesi differenti, di cui 86 in Svizzera.

RISULTATI

I reati sessuali online nei confronti dei minori

La ricerca della letteratura scientifica ha permesso di rilevare alcune caratteristiche principali dei fenomeni in questione secondo gli studi recenti, in particolare per quanto riguarda le vittime, gli autori e il modus operandi, analizzando studi condotti principalmente nei Paesi anglosassoni. A livello svizzero si rileva invece una mancanza di dati. D'altronde, gli indicatori per osservare i fenomeni di reati sessuali online (statistiche della criminalità, sondaggi di vittimizzazione, altre inchieste pubbliche e private) sono recenti e, allo stato attuale, non permettono di fornire un'interpretazione né sull'ampiezza né sulle tendenze della criminalità.

I colloqui con gli esperti hanno tuttavia permesso di identificare alcuni punti a cui prestare attenzione, osservati nella loro pratica, per quanto riguarda l'evoluzione di questi reati, le piattaforme utilizzate e le caratteristiche delle vittime e degli autori.

A livello globale, gli esperti intervistati constatano o presumono un aumento dei reati sessuali online nei confronti dei minori. Tuttavia, questa tendenza non è sempre visibile nelle statistiche, il che fa pensare che l'aumento sia considerato nelle cifre nere della criminalità.

Le piattaforme frequentate dai giovani sono spazi interessanti per gli autori dei reati sessuali online nei confronti dei minori, per entrare in contatto con questi ultimi. Queste piattaforme sono talvolta utilizzate unicamente come punto di aggancio, per poi spostarsi verso un servizio di messaggistica criptato. Non è tuttavia possibile stabilire una lista esaustiva delle piattaforme, poiché queste variano con la moda e i progressi tecnologici. Sono però stati identificati alcuni tipi di piattaforma rilevanti, come le reti sociali, i videogiochi online, i siti per adulti (p. es. siti erotici), i servizi di messaggistica istantanea e il dark web.

Per quanto riguarda le caratteristiche delle vittime e degli autori, non esiste un profilo tipo in senso stretto. I casi di reati sessuali online indicano che le vittime e gli autori provengono da tutte le classi d'età, da tutte le classi sociali ecc. Allo stato attuale, le statistiche di polizia sulla criminalità sessuale presentano una maggioranza di vittime minorenni di sesso femminile e una predominanza di persone imputate adulte e di sesso maschile. Tuttavia, occorre sottolineare che i ricercatori hanno notato un certo numero di problemi di rappresentatività nei dati di polizia: questi permettono una visione solo parziale della criminalità reale, soprattutto nel contesto della delinquenza sessuale. È dunque difficile mettere in evidenza caratteristiche particolari, poiché le informazioni possono essere generalizzate e mal interpretate, soprattutto per i fenomeni più recenti (p. es. live streaming), per i quali le conoscenze accademiche e degli esperti nonché le denunce alle autorità di polizia restano sporadiche.

Gli attori incaricati della protezione dei minori online

In maniera generale, svariati attori sono coinvolti in questa tematica, a livello statale (dipartimenti e uffici di governo, corpi di polizia), associativo, dell'industria (in particolare le imprese private di telecomunicazione) o ancora del contesto scolastico pubblico o privato.

Questi attori si occupano di trattare le questioni legate ai reati sessuali online in funzione del loro campo di responsabilità o del loro settore di competenza. Se il contesto scolastico contribuisce principalmente a insegnare una buona igiene digitale, le associazioni e le fondazioni forniscono

soprattutto consigli e sviluppano piattaforme di aiuto e attività ludiche. In qualità di fornitori di servizi di telecomunicazione, alcune imprese private sono coinvolte nella protezione dei bambini e degli adolescenti proponendo innanzitutto misure tecniche; alcune offrono anche corsi di sensibilizzazione o finanziano studi sull'utilizzo dei media. I dipartimenti e gli uffici del governo sviluppano collaborazioni con altri partner o istituzioni, e misure di sensibilizzazione per il grande pubblico. Per finire, la polizia combina il lavoro di repressione, che include l'individuazione e l'investigazione dei reati sessuali online, con un lavoro di prevenzione grazie a scambi di informazioni, corsi di sensibilizzazione e una presenza online tanto preventiva quanto repressiva.

Le misure rilevate in Svizzera

Nel presente studio si constata lo sviluppo di una molteplicità di misure in Svizzera. Su 86 misure identificate, più della metà è implementata o resa accessibile a livello cantonale o locale. Le iniziative sviluppate in prospettiva nazionale rappresentano poco più di un quarto delle misure identificate. Altre misure hanno infine una portata più regionale.

Le misure rilevate sono raggruppate in quattro categorie: preventive, tecniche, di polizia e giuridiche. Tra le *misure preventive,* la maggior parte delle misure si presenta come offerta di formazione (corsi di sensibilizzazione) o di messa a disposizione di informazioni e consigli (tramite siti internet, opuscoli ecc.). Sono state inoltre rilevate attività ludiche, misure di aiuto e sostegno (senza opzione di trattamento) e una campagna di sensibilizzazione su scala nazionale. Per quanto riguarda le *misure tecniche*, sono stati rilevati software e app di controllo e di blocco proposti da servizi di telecomunicazione e associazioni. Inoltre, vengono messe a disposizione della popolazione piattaforme apposite per segnalare reati online o la scoperta di materiale pornografico proibito (compresa la pornografia infantile) su Internet. Infine, alcune scuole adottano carte di sicurezza per ricordare agli allievi le regole di buona condotta. Per quanto riguarda le *misure di polizia*, alcuni mezzi investigativi non possono essere divulgati pubblicamente per assicurare la continuità del lavoro delle forze dell'ordine. Senza entrare nei dettagli operativi, si può rilevare che il monitoraggio degli annunci del National Center for Missing & Exploited Children (NCMEC), il blocco di siti Internet, le ricerche preventive segrete, le banche dati di polizia nazionali e internazionali nonché le collaborazioni con altre autorità di polizia e/o giudiziarie estere fanno parte degli strumenti e dei metodi di polizia che contribuiscono alla prevenzione e alla lotta contro la delinquenza sessuale online nei confronti dei minori. Infine, le *misure giuridiche* fanno riferimento al diritto penale svizzero in vigore, che considera come criminali i quattro fenomeni analizzati in questo mandato.

Pubblico target delle misure rilevate in Svizzera

Quasi la metà delle misure rilevate è rivolta ai bambini e agli adolescenti. Seguono le misure indirizzate ai genitori. Le iniziative formulate per gli insegnanti e gli altri operatori che lavorano con bambini e adolescenti sembrano poche. Tuttavia, la capacità di azione della prevenzione risulta limitata se non include gli ambienti propri dei bambini e degli adolescenti come gli insegnanti e la comunità in senso più ampio. Inoltre, le misure volte a modificare l'ambiente (le situazioni) sono più rare.

D'altro canto, la maggior parte delle misure di prevenzione rilevate in Svizzera è concepita per le (potenziali) vittime. La prevenzione dovrebbe dunque essere indirizzata anche ai (potenziali) autori, al fine di impedire il passaggio all'atto o la recidiva.

Limitazioni, lacune e spunti di riflessione

Nel quadro del presente studio sono stati messi in evidenza cinque punti a cui prestare attenzione.

- *Lacune nelle conoscenze*: si rileva una mancanza di dati riguardo al cibergrooming, alla sextortion e al live streaming, in particolare per quanto riguarda gli studi accademici. In effetti, gli studi esaminati sui quattro fenomeni di interesse provenivano per la maggior parte dai Paesi anglosassoni. Un potenziamento delle ricerche, anche in Svizzera, permetterebbe di conoscere meglio questi fenomeni e di concepire misure di prevenzione adeguate alla loro evoluzione.
- *Complessità del coordinamento tra gli attori*: in generale, svariati attori si interessano a questa tematica, che sia a livello statale, associativo, dell'industria o del contesto scolastico. Tuttavia, l'approccio settoriale è più diffuso di quello trasversale. Tranne per quanto riguarda l'ambito della polizia, in cui la cooperazione internazionale si è fortemente sviluppata per combattere lo sfruttamento sessuale dei minori su Internet, ci sono margini di miglioramento nelle collaborazioni all'interno dei singoli settori di attività e tra di loro. Sarebbe quindi positivo rafforzare le reti esistenti e la collaborazione tra pubblico e privato, che potrebbe agire come fattore di armonizzazione e di sistematizzazione delle conoscenze e delle competenze.
- *Misure dissociate e piuttosto tradizionali*: soprattutto a causa del fatto che gli attori non collaborano sempre in reti organizzate, si osserva l'implementazione di misure dissociate. D'altra parte, la maggior parte delle misure identificate in Svizzera si presenta come offerta di formazione (sensibilizzazione) o di messa a disposizione di informazioni e consigli (tramite siti internet, opuscoli ecc.), che sono misure relativamente classiche. La prevenzione potrebbe dunque tendere verso iniziative più diversificate associando divertimento e messaggi educativi, accrescendo al contempo la presenza sui canali di comunicazione popolari tra i gruppi target (p. es. per i giovani, le reti sociali e le piattaforme di videogiochi).
- *Approccio orientato principalmente ai giovani e alle (potenziali) vittime*: la maggior parte delle iniziative di prevenzione è indirizzata principalmente ai bambini e agli adolescenti, che sono considerati come gruppo vulnerabile e potenziali vittime. La capacità di azione della prevenzione risulta tuttavia limitata se non include l'insieme degli ambienti del gruppo target. In questo senso, andrebbe privilegiato un approccio olistico. D'altronde, la prevenzione dovrebbe essere indirizzata anche ai (potenziali) autori, al fine di impedire il passaggio all'atto o la recidiva. In questa prospettiva di prevenzione secondaria e terziaria, potrebbe essere rafforzato il sistema di sostegno e aiuto (con e senza opzione di trattamento) alle persone che hanno un'attrazione sessuale per i minori o che hanno commesso un reato sessuale online nei confronti di minori.

- *Difficoltà a individuare le buone pratiche nell'ambito dell'identificazione e della prevenzione*: anche la dispersione delle informazioni può rappresentare un ostacolo per la comprensione e per l'elaborazione di proposte di soluzioni per prevenire e combattere i reati sessuali online. Lo sviluppo di strumenti di informazione, di controllo e di identificazione delle situazioni permetterebbe di migliorare la visione di questi fenomeni e di ottimizzare il processo decisionale a livello strategico e operativo. D'altro canto, dallo studio emerge che è difficile stabilire, da un punto di vista scientifico, quali sono le misure più efficaci. In effetti, le valutazioni sui programmi di prevenzione in materia, in Svizzera e all'estero, sono molto scarse. L'attuazione di processi di valutazione dell'efficacia dei programmi di prevenzione dovrebbe quindi essere incoraggiata e sostenuta al fine di perfezionarli e, se necessario, di creare conoscenze derivanti dalla pratica.

RACCOMANDAZIONI

Sulla base delle informazioni analizzate nel quadro di questo rapporto, sono state formulate dieci raccomandazioni per lavorare sulle prospettive di evoluzione menzionate in precedenza e per migliorare la capacità del sistema svizzero di rispondere a questi fenomeni di reati sessuali online nei confronti dei minori.

21. Incoraggiare e sostenere le ricerche scientifiche sul tema dei reati sessuali online nei confronti dei minori.
22. Sviluppare una strategia nazionale per la prevenzione dei reati sessuali online nei confronti dei minori.
23. Rafforzare la collaborazione tra pubblico e privato per il monitoraggio, lo smistamento dei casi e la condivisione dei dati.
24. Sostenere l'armonizzazione delle basi legali per permettere lo scambio di dati durante le inchieste.
25. Sviluppare misure che associno divertimento e messaggi educativi, accrescendo al contempo la presenza sui canali di comunicazione popolari tra i gruppi target (p. es. per i giovani, le reti sociali e le piattaforme di videogiochi).
26. Assegnare ai minori un ruolo attivo nella concezione e nell'attuazione delle misure di prevenzione.
27. Rafforzare la formazione degli insegnanti e degli operatori attivi nell'ambito della gioventù. Conoscenze più mirate su questi fenomeni permetterebbero loro di seguire e sostenere meglio i bambini e gli adolescenti.
28. Sostenere lo sviluppo e la promozione di una rete di sostegno e aiuto (con e senza opzione di trattamento) per le vittime e i (potenziali) autori.
29. Sviluppare strumenti di informazione, di controllo e di identificazione delle situazioni.
30. Incoraggiare e sostenere la valutazione scientifica dei programmi di prevenzione.

Summary

STUDY REMIT

The Quadranti postulate 19.4111, which the National Council adopted on 20 December 2019, aims to protect minors who are induced to engage in sexual activity via their mobile phone or other devices with photographic or video recording capabilities. It calls on the Federal Council to examine what measures could be taken to prevent children and young people from being exposed to situations where an adult grooms or coerces them to produce pornographic content. The FSIO responded to the postulate by commissioning the School of Criminal Sciences of the University of Lausanne in October 2021 to produce the present report, *Measures to protect children and young people from online sex crimes*.

This commissioned research paper focuses on four online behaviours:

(a) the **online production and distribution of child pornography**, including sexual content that centres on the visual depiction of a child's genitalia for the purpose of sexual arousal;

(b) **cybergrooming** which involves an adult building an online relationship with a child with a view to exploiting them for sexual purposes;

(c) **sextorsion** which involves blackmailing a child with digital content of a sexual nature, such as revealing photos of the minor harvested by the extortionist from social media platforms;

(d) the **livestreaming of sex acts**, i.e. the broadcasting in real time and over the internet of a child performing sex acts or of a third party performing sex acts on a child.

This report is divided into nine chapters. Following the introduction (Chapter 1), Chapter 2 provides an overview of the situation in Switzerland, including the existing legal framework, the prevalence of these four online behaviours based on police crime statistics, and the powers allocated to the police and prosecution authorities. Chapter 3 describes the methodology and Chapter 4 presents the research findings. The latter is further divided into four sections, the first of which sets out the characteristics of these crimes, as well as those of the perpetrators and their victims based on the findings of a review of academic papers from the 2016–2021 period. The second section presents the actors and networks in Switzerland which are involved in the protection of minors. The third section categorises the measures that Switzerland has already introduced (the approaches adopted and target groups) and sheds more light on initiatives implemented in other countries. The final section provides a summary of expert opinions on the evolution of the four online behaviours covered by the study, the responses to them and the main challenges they present, as well as the steps that could be taken to improve the protection of children and young people. The final chapter (Chapter 5) presents a general discussion of the results, the authors' conclusions and recommendations which address each of the questions enumerated in the FSIO call for projects. Chapter 5 also suggests other ideas on how to better protect minors from online sex crimes.

Questions set out in the FSIO call for projects

1.1 In what parts of the internet do online sex crimes occur, and in what context (platform types and chatrooms, types of activity)? What profiles do victims and perpetrators have?

1.2 In Switzerland, what measures have already been implemented at the cantonal, national and international level? Include state and private-sector (industry self-regulation agreements, platform services etc.).

1.3. Who are the main actors and networks (e.g. NEDIK) in Switzerland behind these measures? What is their remit and scope of action?

1.4. Who are these measures aimed at ([potential] perpetrators, underage victims, children and young people, parents, professionals, etc.)?

2.1. What are the possibilities offered by these measures? What are their limitations?

2.2. Which measures have proven to be particularly effective? Are there examples of good practice in Switzerland and in other countries? To what extent are these practices transferable to Switzerland?

2.3. Are there gaps in relation to the protection of minor, and if so, how significant are they?

2.4. What recommendations can be made for Switzerland?

METHODOLOGY

The report used four methods of data collection: 1) a literature review which identified 105 research papers, including 35 literature reviews of empirical research papers, as well as 70 original empirical studies; 2) a structured online questionnaire on actors, initiatives and collaborations. This was distributed among 447 institutions and four school networks covering all 26 Swiss cantons. A total of 134 institutions responded to the questionnaire, including 45 institutions that are actively involved in the protection of minors from cybercrimes. In addition, 58 measures and 22 networks/working groups were identified that seek to protect minors from at least one of the four online behaviours covered by the study; 3) a structured literature review to identify measures introduced in other countries and integrate information on those taken in Switzerland. The analysis identified 188 measures that had been adopted by 29 countries (24 of these measures pertain to Switzerland; 4) 15 interviews, between January and April 2022, with 18 experts (nine women and nine men) from Switzerland and elsewhere on the four online behaviours under consideration, as well as the measures taken to date to protect minors from these criminal activities and how effective they have been. The research team cross-referenced the data collected from these four steps, which identified that 29 countries had implemented a total of 257 measures, 86 of which were taken in Switzerland.

RESULTS

Online sex crimes against minors

From the literature review, the authors were able to identify several key characteristics of the four online behaviours, including the characteristics of the victims and perpetrators of these crimes, and the modus operandi. The majority of the publications in the literature review were carried out in English-speaking countries. The study found that data for Switzerland was scant. The indicators used to map online sex crimes (crime statistics, crime victim surveys and other public and private surveys) are recent and, as they currently stand, do not make it possible to offer any interpretation of either the prevalence and trends in relation to these crimes.

However, the expert interviews revealed several points of interest, which the professionals had observed in practice. These concern the evolution of these forms of criminal activity, the platforms used, as well as the characteristics of both the victims and perpetrators of such crimes.

Overall, the experts who were interviewed state or infer that online sex crimes against minors are on the rise. However, the statistics do not always reflect this, which suggests that a share of these crimes may be going unreported.

Platforms that young people frequent are attractive spaces for perpetrators of online sex crimes to make contact with minors. In some instances, the perpetrators use these platforms to strike up initial contact but subsequently communicate via encrypted messaging services. It was not possible to compile an exhaustive list of platforms due to the fact that they vary according to changing trends and technological advances. However, the study identified the types of platform involved. They include social networks, online gaming sites, adult-only sites (e.g. porn sites), instant messaging services and the dark web.

In terms of victim and perpetrator characteristics, no ‘typical’ profile, in the strictest sense of the term, emerges. The analysis of cases involving online sex crimes found that victims and perpetrators come from all age groups and social classes. Police statistics on sex crimes to date show that most victims are underage females and most defendants are adult males. However, researchers have long highlighted several problems regarding the representativeness of police data, owing to the fact that they do not capture all of the crimes, particularly those of a sexual nature, which have been effectively committed. Caution is therefore required when identifying victim and perpetrator characteristics as there is a risk of generalising and misinterpreting the information, especially information on newer forms of online sex crimes (e.g. livestreaming of sex acts) where scientific and expert knowledge and complaints made to police remain anecdotal.

Child online protection actors

Multiple actors have taken up this issue, at the state (government departments and offices, police forces) and industry (particularly private telecommunications companies) levels, within the voluntary sector and the public and private school community.

The choice of issues related to online sex crimes that they choose to address is based on their respective areas of responsibility or expertise. Schools primarily concern themselves with teaching good cyber hygiene practices, while the voluntary sector (associations and foundations) mainly provide advice

and develop support platforms and play-based activities. In terms of the private sector, a number of telecommunications providers contribute to online child protection efforts principally at the technical level, but they also design e-safety awareness courses and fund research on media use. Government departments and offices develop forms of cooperation with other institutions or partners and measures to raise public awareness. Finally, the police combine their law enforcement duties and work to identify and investigate cases of online sex crimes with preventive efforts, which include information sharing, the running of awareness courses and maintaining an online presence that is geared towards both prevention and suppression.

Measures taken in Switzerland

The present reports find that a wide range of measures have already been developed in Switzerland. Of the 86 measures that the research identified, more than half are implemented or accessible at the cantonal level, and in some cases at local level as well. Over a quarter of the 86 measures concern initiatives that are national in scope. A further set of measures identified by the research are region-specific.

These measures fall into four categories: preventive, technical, police and legal. The majority of measures in the *preventive* category revolve around training (e.g. awareness courses) or the provision of information and advice (e.g. websites and brochures), but also include play-based activities, support (without treatment options) and national public information campaigns. Measures in the *technical* category include control and blocking software/applications provided by telecommunication services or the voluntary sector. Another measure in this category is the creation of internet platforms where the public can report cybercrimes or prohibited forms of pornography, including child pornography, which they have encountered online. Finally, a number of schools have adopted e-safety charters that provide students with a list of good practices when using the internet. As for *police measures*, certain investigative methods cannot be publicly disclosed to ensure that the ongoing work of law enforcement is not compromised in any way. Without going into the operational details, the research identified the following law enforcement tools and measures to prevent and combat online sex crimes against minors: monitoring of suspicious activity alerts from the National Center for Missing & Exploited Children (NCMEC), website blocking, preventive covert searches, national and international police databases, and collaboration with other foreign police/judicial authorities. Finally, *legal measures* cover the legislation currently in force in Switzerland criminalising the four online behaviours covered by the study.

Target groups of the measures identified in Switzerland

Almost half of the measures are aimed at children and young people. The second largest target group are parents. The study found few initiatives that were designed specifically for teachers and other professionals who work with children and young people. The capacity for preventive action is limited if it does not include the child or young person's social environment, i.e. teachers and the wider community. Measures that tend to change the environment, i.e. situations, are rarer.

Most prevention measures in Switzerland focus exclusively on (potential) victims. Measures are therefore needed that target (potential) perpetrators specifically with a view to prevent first-time and repeat offences.

Limitations, gaps and new avenues to explore

The study identifies five key points:

- *Gaps in knowledge*: there is a lack of data and research in Switzerland on cybergrooming, sextortion and the livestreaming of sex acts. Most of the research which this study draws on was carried out in English-speaking countries. More research is needed generally and in Switzerland specifically to improve our understanding of the four types of online crimes covered by the study and to facilitate the development of prevention measures that are in sync with trends in relation to these phenomena.
- *Coordination complexity*: multiple actors – state, voluntary sector, industry, schools – have addressed this issue. Yet, a silo approach remains more common than a cross-cutting one. With the exception of the police, where there is extensive international cooperation on combatting the sexual exploitation of minors online, collaboration within and between the different fields of activity could be improved. To facilitate this, steps should be taken to bolster existing networks as well as public-private partnerships which could help to advance the harmonisation and systematisation of knowledge and skills.
- *Disjointed and unoriginal approaches to prevention*: the measures which have been implemented to date tend to be disjointed, due in particular to the factor that the actors concerned do not always organise themselves into networks. Most of the measures in Switzerland that the study identified adopt a relatively conventional approach to prevention, i.e. centred around training (e.g. awareness-raising) and the provision of information and advice (e.g. websites and brochures). Future prevention initiatives should therefore seek to adopt a more diversified approach that combines entertainment and education, as well as raise their visibility on communication channels popular with the given target groups (e.g. for young people, social networks and online gaming platforms).
- *Focus on young people and (potential) victims*: most prevention initiatives are aimed at children and young people, because they are regarded as a vulnerable group and potential victims. However, the capacity for preventive action will be limited if such measures do not include the child's environment. A more holistic approach is called for here. Furthermore, efforts should also target the (potential) perpetrators in order to prevent them from becoming first-time/repeat offenders. From the perspective of secondary and tertiary prevention, steps should be taken to reinforce the system of that supports and helps (with and without treatment options) individuals who are sexually attractive to minors or who have already committed an online sex crime against minors.

- *Difficulties with the identification of good detection and prevention practices*: information spread can also be an obstacle to improving understanding and proposing solutions intended to prevent and combat online sex crimes. The development of intelligence, monitoring and detection tools would make it possible to generate a clearer and more detailed picture of these phenomena and optimise strategic and operational decision-making. At the same time, the study shows that it is difficult to establish, from a scientific perspective, which measures are the most effective. Evaluations of prevention programmes in this field lack relevance, both in Switzerland and elsewhere. The implementation of processes to evaluate the effectiveness of prevention programmes should therefore be encouraged and supported in order to improve them, where necessary, and to generate practice-led knowledge from practice.

RECOMMENDATIONS

The authors have formulated 10 recommendations based on the study findings. They this report, ten recommendations have been formulated to work on the above-mentioned perspectives of development and to improve the capacity of the Swiss system to respond to the issue of online sex crimes against children.

31. Encourage and support academic research on online sex crimes against minors.
32. Develop a national strategy on the prevention of online sex crimes against minors.
33. Strengthen public-private partnerships for monitoring, screening and data sharing.
34. Support the harmonisation of legal bases to enable data-sharing during the investigative process.
35. Develop measures that are designed to simultaneously educate and entertain, and increase visibility on communication channels that are popular with the target groups (social networks and online gaming platforms, in the case of young people, for example).
36. Active participation of minors in the design and implementation of prevention measures.
37. Step up training for teachers and youth workers. The greater their knowledge is, the better the mentoring and support they offer the children and young people in their care.
38. Advocate for the development and promotion of a support and assistance network (with and without treatment options) for victims and (potential) perpetrators.
39. Develop intelligence, monitoring and detection tools**.**
40. Encourage and support the scientific evaluation of prevention programmes.

1. Introduction

L'utilisation de nouvelles technologies offre de multiples opportunités mais elle présente également divers dangers pour une population adolescente manquant de connaissances ou de ressources, qu'elles soient personnelles ou techniques, pour anticiper les risques liés à l'utilisation d'Internet ou des médias sociaux. Différents comportements répréhensibles visant les enfants ou adolescents, et plus particulièrement leur intégrité sexuelle, ont fait surface à la suite de l'arrivée de personnes de jeune âge dans la sphère numérique. Ces préoccupations ont été relevées par plusieurs États cherchant à protéger ou soutenir les groupes les plus vulnérables, tels que les enfants et les jeunes.

Le 20 décembre 2019, le Conseil national a adopté le postulat 19.4111 Quadranti visant à protéger les enfants incités à se livrer à des actes d'ordre sexuel à l'aide de leur téléphone ou autres appareils permettant une prise de vue photographique ou vidéo. Ce postulat demande au Conseil fédéral d'examiner quelles sont les mesures appropriées pour éviter que les enfants et les jeunes se retrouvent dans des situations dans lesquelles ils seraient incités ou forcés par un adulte à produire du matériel pornographique. Dans ce cadre, le Conseil fédéral a chargé le Département fédéral de l'intérieur, et plus particulièrement l'Office fédéral des assurances sociales (OFAS), d'étudier cette problématique et de rédiger un rapport. Le 21 juillet 2021, l'OFAS a publié un appel d'offres pour la réalisation d'une étude scientifique qui sert de base pour le rapport du Conseil fédéral en réponse au postulat.

En octobre 2021, l'OFAS a retenu l'Ecole des sciences criminelles de l'Université de Lausanne pour ce mandat. Ce dernier a pour objectif d'apporter une vision d'ensemble des acteurs et des initiatives entreprises dans le domaine de la protection des enfants et des jeunes contre les cyber-délits sexuels.

Le terme « initiative » est ici défini comme tout type d'activités d'intervention (par exemple, campagne, dispositif, formation) et de coordination (réseaux, groupe de travail). Il s'agit ainsi de relever quelles sont les initiatives prometteuses qui existent et quelles sont les possibilités d'amélioration, tout comme les limites, des initiatives mises en place en Suisse et en Europe pour protéger les jeunes et les enfants de la cybercriminalité sexuelle en ligne. Finalement, l'étude vise à formuler des recommandations pour la Suisse, tout en répondant aux questions formulées dans l'appel d'offres.

Le mandat se focalise sur quatre comportements en ligne spécifiques :

(e) la **production ou distribution de matériel pédopornographique via Internet**, incluant notamment les représentations de contenus sexuels, focalisées sur les organes sexuels d'un enfant et ayant pour but de susciter une excitation sexuelle ;

(f) le **cyber grooming** – ou pédopiégeage – consistant à entrer en contact avec un enfant sur Internet à des fins sexuelles ;

(g) la **sextorsion** consistant à faire chanter l'enfant suite à l'acquisition de matériel numérique de type sexuel, comme le fait de se procurer des photos osées d'un mineur au travers de réseaux sociaux ;

(h) le **live-streaming d'actes d'ordre sexuel** consistant à diffuser en direct des actes d'ordre sexuel effectués par l'enfant lui-même ou par une personne tierce sur l'enfant.

Même si par ces délits l'on distingue des comportements différents, il est important d'avoir une vision d'ensemble sur ces quatre phénomènes étant donné leur degré d'interdépendance. Par exemple, dans une situation de cyber grooming, l'auteur peut chercher à obtenir des images à caractère sexuel qu'il distribuera ensuite à ses pairs, se rendant ainsi coupable de distribution de matériel pédopornographique.

Le présent rapport est structuré en neuf chapitres. Après l'Introduction (chapitre 1), le contexte suisse est exposé de manière succincte au chapitre 2, en établissant le cadre juridique applicable, l'ampleur des phénomènes enregistrés à travers la statistique policière de la criminalité, ainsi que la répartition des compétences entre les diverses autorités policières et de poursuite pénale. Après avoir illustré la méthodologie utilisée au chapitre 3, les résultats de l'étude sont présentés selon quatre axes au sein du chapitre 4. Le premier introduit, sur la base d'une revue de littérature scientifique, des informations sur les caractéristiques de ces délits ainsi que celles des auteurs et victimes sur la base des études récentes (2016-2021). Le deuxième propose un recensement des acteurs suisses actifs dans la protection des enfants et des jeunes, et de leurs collaborations. Le troisième axe décrit une typologie de mesures existantes en Suisse, tout en apportant un éclairage complémentaire en lien avec des initiatives repérées dans d'autres pays. Enfin, le dernier axe relaye l'avis d'experts sur l'évolution des quatre phénomènes étudiés, les réponses qui y sont données, ainsi que les perspectives en matière de protection des enfants et des jeunes. Pour terminer, après une discussion générale sur l'ensemble des résultats (chapitre 5), la conclusion et les recommandations de ce rapport répondent aux questions soulevées dans l'appel d'offres de l'OFAS.

Questions formulées dans l'appel d'offres de l'OFAS

1.1. Où sur Internet et dans quelles situations (types de plateformes et de chats, types d'activités) les différents cyber-délits sexuels ont-ils lieu ? Quelles sont les caractéristiques des victimes et des agresseurs ?

1.2. Quelles mesures existent en Suisse au niveau cantonal, national et international ? Outre les mesures étatiques, les mesures du secteur privé doivent également être incluses (accords d'autorégulation des secteurs, services de plateforme, etc.).

1.3. Qui sont les acteurs et réseaux (par ex. NEDIK) principaux qui proposent des mesures en Suisse ? Quel est leur champ de responsabilité et d'action ?

1.4. À qui s'adressent ces mesures ([potentiels] auteurs du crime, victimes mineures, enfants et jeunes, parents, professionnels, etc.) ?

2.1. Quelles sont les possibilités et les limites de ces mesures ?

2.2. Quelles mesures se montrent particulièrement efficaces ? Peut-on identifier des exemples de bonne pratique en Suisse et à l'étranger ? Dans quelle mesure ces dernières peuvent-elles être applicables en Suisse ?

2.3. Dans quelle mesure existe-t-il des lacunes ?

2.4. Quelles recommandations peuvent être formulées pour la Suisse ?

2. Contexte suisse

Ce chapitre apporte quelques éléments permettant de dresser un cadre général relatif aux cyber-délits sexuels dans le contexte helvétique. Pour commencer, les premiers chiffres sur l'ampleur des quatre phénomènes d'intérêt sont présentés. Ensuite, le cadre juridique entourant ces comportements est exposé en soulignant principalement les bases légales pénales applicables, accompagnées de quelques considérations issues de la jurisprudence. Enfin, la répartition des compétences en matière d'investigation et de poursuite pénale est abordée.

2.1 Quelques chiffres sur la cyberdélinquance sexuelle

Afin de mesurer l'ampleur d'un phénomène criminel ou ses caractéristiques, l'on recourt habituellement à trois types d'indicateurs : les statistiques policières de la criminalité, les sondages de victimisation, et les rapports d'activité d'institutions ou d'entreprises. Toutefois, bien que ces données apportent des renseignements précieux à la compréhension de la criminalité, elles dressent un état de situation incomplet. En effet, chacun de ces indicateurs souffrent de problèmes de validité et/ou fiabilité[1]. Le principal d'entre eux est le chiffre noir, c'est-à-dire la criminalité non découverte ou non dénoncée. En effet, un grand nombre d'infractions pénales n'est pas reporté aux autorités compétentes ou n'est pas découvert par la police. Or, plusieurs auteurs s'accordent pour dire que la mesure de la cybercriminalité (aussi appelée criminalité numérique ou criminalité informatique[2]) comporte des challenges supplémentaires par rapport à la criminalité dite traditionnelle (ou criminalité physique)[3], et que le chiffre noir est encore plus grand en ce qui concerne la cybercriminalité[4].

D'autre part, la composante cyber est encore peu présente dans les sondages de victimisation traditionnels adressés à une large part de la population, et ce d'autant plus en matière de cyber-délits sexuels. Ces dernières années, quelques sondages, menés notamment auprès des citoyens des villes de Zurich et de Lugano, ont introduit la criminalité numérique dans leurs questionnements, mais en se limitant aux cyber-délits économiques[5]. En revanche, le Sondage suisse au sujet des expériences et opinions sur les délits 2022, commandé par la Conférence des commandantes et des commandants des polices cantonales suisses (CCPCS) et mené à l'échelle nationale auprès d'une population âgée de plus de 15 ans, prévoit d'introduire des questions sur le harcèlement sexuel, les menaces et l'extorsion en ligne. En attendant d'obtenir ce type de données, certaines études portant sur l'utilisation d'Internet peuvent fournir des renseignements sur la thématique (*infra*, ch. 2.1.2).

De ce fait, il est difficile de mesurer la cybercriminalité et d'établir une vision claire de l'ampleur et des caractéristiques de ce type de comportements criminels. Tout en gardant à l'esprit ces difficultés méthodologiques, et en prenant les précautions nécessaires, nous présentons dans les sections

[1] Aebi (2006).
[2] Alors que ces termes sont parfois utilisés comme des synonymes, certains praticiens ou auteurs opèrent une distinction. Par exemple, selon la procureure du Ministère public de la Confédération Sandra Schweingruber, la criminalité informatique fait référence aux nouveaux comportements qui n'existaient pas avant le développement d'Internet, à savoir les infractions « dirigées contre les données et les ordinateurs » (Schwegler, 2022b). Tandis que la criminalité numérique englobe les infractions déjà connues mais pour lesquelles Internet fournit un nouveau moyen de les perpétrer. Cette délimitation s'apparente à une typologie populaire relevée dans la littérature scientifique internationale, qui sépare les « cyber-dependent crime » des « cyber-enabled crime » (McGuire & Dowling, 2013).
[3] Aebi, Caneppele, et Molnar (2022); Caneppele et Aebi (2019); Côté, Bérubé, et Dupont (2016); da Silva, Burkhardt, et Caneppele (2022).
[4] Gercke (2012); Reep-van den Bergh et Junger (2018).
[5] Baier (2019); Caneppele, Milani, Burkhardt, da Silva, et Aebi (2019).

suivantes les premiers chiffres accessibles pour la Suisse tirés des statistiques policières ou des sondages d'utilisation d'Internet.

2.1.1 Statistiques policières de la criminalité

Depuis l'année 2020, l'Office fédéral de la statistique (OFS) publie également des données sur la cybercriminalité dans le cadre du rapport annuel sur les statistiques policières de la criminalité (SPC). Ainsi, au moment de rédiger ce rapport, seules les données pour les années 2020 et 2021 sont disponibles.

Au-delà du nombre d'infractions enregistrées par la police, la SPC nous informe sur le taux d'élucidation, ainsi que sur certaines caractéristiques relatives aux prévenus et aux victimes (nombre, tranches d'âge, sexe, statut de séjour).

La SPC répartit les infractions dites « cyber » en cinq grands domaines, parmi lesquels celui des cyber-délits sexuels[6]. Ces derniers sont ensuite catégorisés en quatre types d'infractions, similaires à nos phénomènes d'intérêt pour la présente étude. En effet, la SPC recense toutes les infractions enregistrées par la police, peu importe l'âge de la personne prévenue et de la victime. En revanche, cette étude se focalise principalement sur les cyber-délits sexuels commis par des adultes à l'encontre de mineurs.

Le Tableau 1, ci-dessous, nous renseigne tout d'abord sur le nombre de cyber-délits sexuels enregistrés par la police en 2020 et 2021. Au total, ils sont au nombre de 2572 pour l'année 2021, ce qui correspond à 0,38% des infractions au Code pénal enregistrées et à 8,5% de la cybercriminalité. Dans l'ensemble, le nombre de cyber-délits sexuels enregistrés est demeuré stable entre 2020 et 2021, une légère baisse de 2% étant indiquée.

Tab. 1 – Nombre de cyber-délits sexuels enregistrés par la police en 2020 et 2021

	2020		2021		Différence
	Nb infractions	% élucidations	Nb infractions	% élucidations	
Cyber-délits sexuels	2612	94%	2572	92,9%	-2%
Pornographie interdite	2338	96,8%	2243	95,9%	-4%
Grooming	130	80%	141	85,1%	8%
Sextorsion	109	49,5%	153	56,2%	40%
Live-streaming	35	94,3%	35	97,1%	0%

Sources : Office fédéral de la statistique OFS, Statistique policière de la criminalité (SPC). Rapport annuel 2020 et 2021 des infractions enregistrées par la police.

En revanche, si l'on s'attarde sur les types de cyber-délits sexuels, des différences plus significatives sont soulignées. La pornographie interdite[7] est le type d'infraction prédominant en matière de cyber-délits sexuels (87,2%). Suivent ensuite la sextorsion et le grooming dans une proportion similaire (respectivement 5,95% et 5,48%) ; le live-streaming étant l'infraction la moins détectée (1,36%). Les taux entre l'année 2020 et 2021 varient également en fonction du type d'infraction. Alors que le

[6] Les trois autres catégories sont la criminalité économique, les cyber-atteinte à la réputation et les pratiques déloyale, et le commerce illégal sur le Dark web.
[7] Au sens de l'article 197 al. 2 CP, la pornographie interdite inclut les objets ou les représentations « […] ayant comme contenu des actes d'ordre sexuel avec des animaux, des actes de violence entre adultes ou des actes d'ordre sexuel non effectifs avec des mineurs […] ».

nombre d'infraction pour pornographie interdite est en légère baisse (-4%), les chiffres pour le grooming, et plus encore pour la sextorsion, sont en augmentation (respectivement +8% et +40%). Il faut préciser que les pourcentages de changement sont à interpréter avec prudence lorsque les chiffres absolus sont relativement petits. En ce sens, l'augmentation de 40% des délits de sextorsion représente, en valeur absolue, une hausse de 44 cas.

Une autre information reportée dans le Tableau 1 est le taux d'élucidation. De manière générale, le taux d'élucidation en matière de cyber-délits sexuels est très élevé (92,9% en 2021). A nouveau des différences sont observées entre les différents types d'infractions. Tandis que les infractions de pornographie interdite, de live-streaming et de grooming portés à la connaissance de la police semblent être élucidés dans la majorité des cas (variation entre 85,1% et 97,1% en 2021), le taux d'élucidation relatif à la sextorsion est plus faible. En effet, il ressort qu'environ une infraction sur deux n'est pas résolue (56,2%)[8].

Enfin, la SPC nous informe également sur certaines caractéristiques socio-démographiques des victimes (personnes lésées) et des prévenus des infractions enregistrées. Le premier constat est le nombre plutôt bas de personnes lésées. Pour l'ensemble des 2572 cyber-délits sexuels enregistrés en 2021, seules 331 victimes ont été identifiées[9]. Alors que pour la sextorsion la victime semble avoir été identifiée, il ressort que cette tâche est bien plus complexe en matière de pornographie interdite. Ceci peut s'expliquer du fait que dans une affaire de sextorsion, la victime est vraisemblablement au courant dès lors qu'un tiers tente de l'extorquer, et que c'est elle qui va dénoncer l'acte à la police. En revanche, en matière de pornographie interdite, d'une part, la personne figurant sur le matériel pornographique n'a pas forcément connaissance de l'existence de ce matériel et, d'autre part, ce type de matériel peut être distribué et échangé à de nombreuses reprises.

Si l'on regarde l'âge des personnes lésées, le Tableau 2 relève qu'un peu moins des ¾ des victimes de cyber-délits sexuels sont des personnes mineures (72,6%). La tranche d'âge la plus touchée est celle des 10-15 ans. Cette tendance est présente pour chacun des comportements, à l'exception de la sextorsion pour laquelle la proportion de victimes mineures est plus faible, mais demeure tout de même importante (53,2%)[10].

[8] Selon deux experts interviewés dans le cadre de cette étude, cette observation peut s'expliquer du fait que, en matière de sextorsion, l'auteur se trouve souvent à l'étranger et use de techniques sophistiquées rendant son identification plus laborieuse.
[9] Pour les données relatives à l'année 2020, nous renvoyons le lecteur à l'Annexe A.
[10] La proportion plus élevée d'adultes victimes de sextorsion – par rapport aux trois autres délits – s'explique par le fait que l'extorsion peut notamment consister en une demande d'argent ou de matériels pornographiques supplémentaires (*infra*, ch. 2.2.3). Or, la première variante est davantage pratiquée envers des victimes adultes (Wolak, Finkelhor, Walsh, & Treitman, 2018; Wolak & Finklelhor, 2016), dès lors qu'elles disposent de moyens financiers plus importants.

Tab. 2 – Caractéristiques des personnes lésées par un cyber-délit sexuel enregistré par la police en 2021

	Total victimes	Tranches d'âge						Sexe	
		<10	10-15	15-17	18-19	20-25	25+	Masculin	Féminin
Cyber-délits sexuels	311	18	134	74	20	22	40	82	227
Pornographie interdite	129	10	62	24	5	10	17	34	94
Grooming	69	4	42	23	0	0	0	16	53
Sextorsion	109	0	31	27	14	12	23	28	80
Live-streaming	10	4	3	2	1	0	0	5	5

Source : Office fédéral de la statistique OFS, Tableau 19.02.09.01.03, Criminalité numérique : Modes opératoires de criminalité numérique et personnes lésées, Suisse, Année 2021.

Une autre caractéristique décrite dans le Tableau 2 est le sexe des victimes. Sur les 311 victimes identifiées en 2021, 73% sont de sexe féminin. Cette prédominance de victimes féminines est observée pour tous les types de cyber-délits sexuels, sauf pour le live-streaming. En effet, la proportion de victimes de sexe masculin et féminin est égale. Néanmoins, il convient de souligner à nouveau le nombre très faible de cas enregistrés de live-streaming.

Dans le Tableau 3, ci-dessous, nous retrouvons les mêmes informations mais concernant cette fois-ci les personnes prévenues pour un cyber-délit sexuel enregistré par la police en 2021. La première observation se réfère au nombre de personnes prévenues, qui est bien plus élevé que le nombre de victimes identifiées, et plus particulièrement pour les prévenus de pornographie interdite[11]. Quant à l'âge, 60% des personnes prévenues sont âgées de 18 ans ou plus. Cette tendance se retrouve pour la pornographie interdite, le grooming et le live-streaming (respectivement, 60,5%, 66,3% et 68%). Les tranches d'âge principalement concernées sont les 25-34 ans et 35-49 ans. Alors que pour la sextorsion, un peu moins de la moitié des personnes prévenues sont des adultes (46%). La seconde partie du tableau indique que la presque totalité des personnes prévenues pour de cyber-délits sexuels sont de sexe masculin (88,4% à 94% selon le type de délit).

[11] Plusieurs hypothèses peuvent être formulées pour expliquer le décalage entre le nombre de personnes prévenues et le nombre de personnes lésées en matière de pornographie interdite : 1) une image peut être reproduite et transférée à plusieurs reprises, donc le détenteur du matériel n'est pas forcément à connaissance de l'identité de la victime ; 2) la mondialisation du marché permet aux producteurs de matériel de cibler des victimes dans des continents différents rendant ainsi le travail d'identification des victimes plus ardu ; 3) les images ne dévoilent pas toujours le visage de la victime ou peuvent faire l'objet d'une manipulation ultérieure ce qui complexifie le processus d'identification.

Tab. 3 – Caractéristiques des personnes prévenues pour un cyber-délit sexuel enregistré par la police en 2021

	Total prévenus	Tranches d'âge							Sexe	
		<18	18-19	20-24	25-34	35-49	50-69	70+	Masculin	Féminin
Cyber-délits sexuels	1816	721	118	198	271	279	209	20	1628	188
Pornographie interdite	1690	667	108	180	260	260	195	20	1516	174
Grooming	83	28	5	10	13	16	11	0	75	8
Sextorsion	43	23	7	7	1	0	4	1	38	5
Live-streaming	19	6	0	3	2	4	4	0	18	1

Source : Office fédéral de la statistique OFS, Tableau 19.02.09.01.02, Criminalité numérique : Modes opératoires de criminalité numérique et personnes prévenues, Suisse, Année 2021.

Pour conclure, il convient de souligner encore deux points d'attention sur les statistiques policières de la criminalité. Dès lors que seules les données de deux années sont publiées, il convient d'interpréter les chiffres présentés avec une grande prudence. D'une part, sans comparatif pour la période antérieure à 2020, il n'est pas possible d'interpréter des tendances quant à l'évolution de ces phénomènes criminels. En effet, en matière d'analyses longitudinales, il est généralement recommandé de disposer des données pour 10 années consécutives afin de pouvoir formuler des constats valides. D'autre part, ces premières données publiées en matière de cybercriminalité s'inscrivent dans une période toute particulière, à savoir la pandémie du coronavirus (Covid-19) débutée en 2020. Cette crise sanitaire a engendré des changements dans le style de vie, dont une présence accrue, et parfois non supervisée, au logement, ainsi qu'un accès accru aux outils numériques, ce qui a facilité la commission de comportements répréhensibles sur Internet. Plusieurs organisations ont fait part de leur inquiétude, notamment en ce qui concerne l'exploitation sexuelle des enfants[12].

2.1.2 Sondages sur l'utilisation d'Internet

Comme relevé précédemment, les sondages de victimisation sont encore peu investis dans le domaine de la cybercriminalité. Toutefois, les études spécialisées sur l'utilisation d'Internet par les enfants et les jeunes nous renseignent sur leurs habitudes cybernétiques et peuvent contribuer à la compréhension des cyber-délits sexuels. Pour la Suisse, les résultats de l'étude JAMES conduite par la ZHAW et de l'étude EU Kids online Suisse conduite par la HEP de Schwyz sont disponibles.

a) Etude JAMES 2020 et JAMES focus 2014-2020[13]

L'étude JAMES est menée tous les deux ans, la dernière datant de 2020[14], et plus précisément lors de la première vague de la pandémie Covid-19. En complément, une étude JAMES focus, publiée en 2021, offre une rétrospective sur l'évolution des activités de loisirs médias entre 2014 et 2020[15].

L'étude de 2020 se fonde sur les réponses de 953 jeunes âgés de 12 à 19 ans vivant en Suisse. Les résultats indiquent que les activités de loisirs médias les plus courantes sont l'utilisation du portable (99%), l'utilisation des services Internet, écouter de la musique, l'utilisation des réseaux sociaux

[12] EUROPOL (2020).
[13] Retour sur une décennie d'études sur la jeunesse et les médias.
[14] Bernath et al. (2020).
[15] Waller et al. (2021).

(92%), et regarder des vidéos sur Internet. Les jeux vidéo sont moins souvent utilisés, avec 34% des jeunes en faisant usage. Les tendances entre filles et garçons sont assez similaires pour l'utilisation du portable, des services Internet et des réseaux sociaux. En revanche, il y a davantage de filles qui écoutent de la musique que de garçons (96% vs 89%). Au contraire, les garçons sont plus nombreux à regarder des vidéos sur Internet ou à jouer à des jeux en ligne que les filles (94% vs 76% ; 93% vs 56%)[16].

L'offre des médias numériques étant en croissance permanente, il est pertinent de connaître ceux qui sont le plus utilisés par les jeunes. Si l'on s'intéresse plus précisément aux réseaux sociaux, les plus populaires en 2020 sont Instagram (93% des jeunes ont un compte), Snapchat (91%) et Tiktok (74%)[17]. Quant à la popularité de la plateforme Facebook, elle tend à diminuer au fil des années au profit d'Instagram (50%)[18]. Quant aux canaux de communication directe, l'application WhatsApp satisfait la majorité des jeunes[19]. Enfin, les trois jeux favoris sont Call of Duty, Fortnite et Minecraft.

L'étude aborde également certains comportements relatifs à la sexualité et aux médias. Tout d'abord, que ce soit les réseaux sociaux, les plateformes de messagerie ou les jeux en ligne, ces médias offrent la possibilité d'entrer en contact avec des personnes inconnues[20]. Il ressort que 40% des jeunes ont déjà rencontré dans la vraie vie une personne étrangère dont ils avaient fait la connaissance sur Internet, les filles légèrement plus que les garçons (44% vs 35%). En outre, parmi les joueurs en ligne, 45% d'entre eux jouent avec d'autres personnes au moins une fois par semaine. En parlant de cyberharcèlement, l'étude révèle que 44% des participants indiquent avoir déjà été sollicités sur Internet par un inconnu – qu'il s'agisse d'un mineur ou d'un adulte – ayant des intentions sexuelles indésirables. Cette pratique s'apparente donc au cyber grooming que nous traitons dans le présent mandat. Les filles sont significativement plus nombreuses à rapporter cette situation que les garçons (55% vs 28%), de même que les jeunes âgés de 16-17 ans. À ce sujet, la rétrospective 2014-2020 met en lumière que le taux de jeunes reportant ce type de comportement était moindre en 2014 (19%)[21] .

b) Etude EU Kids online

La seconde étude, EU Kids online Suisse, a été menée en 2019 auprès de 1026 jeunes âgés de 9 à 16 ans de Suisse alémanique et Suisse romande[22] . Cette étude aborde notamment le type d'activités menées sur Internet, ainsi que certains risques auxquels les jeunes ont pu être confrontés. Les résultats montrent que la majorité des jeunes écoutent de la musique (77%) ou regardent des vidéos sur Internet (75%) au moins une fois par semaine. L'utilisation des réseaux sociaux est également une activité très fréquente, dès lors que 59% s'en servent au moins une fois par semaine, de même que le fait de communiquer avec des amis ou des membres de la famille (56%), et d'échanger des messages sur les réseaux sociaux (56%). Viennent ensuite les jeux en ligne (55%), et pour terminer l'utilisation d'Internet pour des travaux scolaires (53%). Il ressort également de l'étude que 35% des participants ont déjà été confrontés à une représentation à caractère sexuel (images, photos ou vidéos). En ce qui

[16] Bernath et al. (2020).
[17] Bernath et al. (2020).
[18] Waller et al. (2021).
[19] Bernath et al. (2020).
[20] Bernath et al. (2020).
[21] Waller et al. (2021).
[22] Hermida (2019).

concerne le fait d'avoir des contacts avec des personnes qu'ils ne connaissent pas personnellement, ils sont 34% à reporter ce type de contacts. Enfin, 21% des enfants ont déjà été sollicités pour fournir des informations à caractère sexuel, alors qu'ils ne le voulaient pas. Ces trois types de comportements ou de situations sont davantage signalés par les jeunes de 15-16 ans que par les enfants plus jeunes. Alors qu'une proportion légèrement plus élevée de fille a reporté des actes de grooming que les garçons (24% vs 18%), ainsi que le fait d'avoir des contacts avec un inconnu (33% vs 35%), les garçons sont légèrement plus nombreux que les filles à avoir été confrontés à des images à caractère sexuel (39% vs 32%). Nous sommes néanmoins dans l'incapacité de dire si ces différences sont significatives.

Ces deux études apportent un éclairage sur les habitudes des jeunes dans leur utilisation d'Internet et des différents médias. Ces informations sont précieuses pour le développement de méthodes de prévention, notamment en lien avec le cyber grooming et les plateformes fréquentées par les mineurs. Néanmoins, ces éléments devraient être complétés par des sondages spécifiques à la question des cyber-délits sexuels, et de la cybercriminalité en général.

2.2 Cadre légal

Les quatre phénomènes étudiés dans ce rapport sont des délits sexuels, qui sont criminalisés par le Code pénal suisse. Dans cette section, nous énonçons les bases légales actuelles pouvant trouver application dans des situations de pédopornographie, cyber grooming, sextorsion et live-streaming. Cet exposé n'a pas pour vocation de fournir une analyse juridique exhaustive des dispositions légales et de leur application, mais plutôt d'apporter un cadre général informatif quant à la réglementation pénale en la matière.

La Suisse a notamment ratifié plusieurs conventions internationales, qu'elle se doit dès lors de respecter en adaptant si nécessaire ses normes légales internes. En lien avec la thématique à l'étude, nous mentionnons notamment la Convention de Budapest[23] (ou Convention sur la cybercriminalité) et la Convention de Lanzarote (Convention du Conseil de l'Europe portant sur la protection des enfants contre l'exploitation et les abus sexuels)[24].

De plus, il est important de mentionner que le droit pénal suisse fait actuellement l'objet d'une révision, touchant notamment les infractions sexuelles. Dès lors que certaines dispositions qui nous intéressent sont abordées dans le cadre de cette révision, nous y faisons également référence[25].

2.2.1 Production et distribution de matériel pédopornographique via Internet

La production et la distribution de matériel pédopornographique via Internet sont réglementées par l'article 197 CP, présenté ci-dessous, qui criminalise certaines formes de pornographie[26]. En effet, plusieurs comportements délictueux protégeant des biens juridiques distincts sont énoncés dans cette disposition composée de neuf alinéas. Le comportement délictuel peut se matérialiser par la

[23] RS 0.311.43. Entrée en vigueur en Suisse le 1er janvier 2012.
[24] RS 0.311.40. Entrée en vigueur en Suisse le 1er juillet 2014.
[25] Il est à préciser que les éléments abordés dans le cadre de l'actuelle révision du droit pénal ne sont pas définitifs. La Commission des affaires juridiques du Conseil des Etats a publié son rapport le 18 février 2022 et le Conseil fédéral a adopté son avis sur le rapport de la CAJ-E le 13 avril 2022 (voir FF2022 1011). Le débat a également eu lieu au Conseil des Etats les 7 et 13 juin 2022. Le projet est actuellement en discussion à la Commission des affaires juridiques du Conseil national.
[26] En matière de production de matériel pédopornographique, d'autres infractions contre l'intégrité sexuelle pourraient être retenues dépendant des faits survenus (art. 187 à 193 CP).

production, la distribution, la possession, et la consommation de matériel pornographique ou encore par le recrutement de mineur en vue de produire du contenu pornographique.

Article 197 – Pornographie

1 Quiconque offre, montre, rend accessibles à une personne de moins de 16 ans ou met à sa disposition des écrits, enregistrements sonores ou visuels, images ou autres objets pornographiques ou des représentations pornographiques, ou les diffuse à la radio ou à la télévision, est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

2 Quiconque expose ou montre en public des objets ou des représentations visés à l'al. 1, ou les offre à une personne sans y avoir été invité, est puni de l'amende. Quiconque, lors d'expositions ou de représentations dans des locaux fermés, attire d'avance l'attention des spectateurs sur le caractère pornographique de celles-ci n'est pas punissable.

3 Quiconque recrute un mineur pour qu'il participe à une représentation pornographique ou favorise sa participation à une telle représentation est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

4 Quiconque fabrique, importe, prend en dépôt, met en circulation, promeut, expose, offre, montre, rend accessible, met à disposition, acquiert, obtient par voie électronique ou d'une autre manière ou possède des objets ou représentations visés à l'al. 1, ayant comme contenu des actes d'ordre sexuel avec des animaux, des actes de violence entre adultes ou des actes d'ordre sexuel non effectifs avec des mineurs, est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. Si les objets ou représentations ont pour contenu des actes d'ordre sexuel effectifs avec des mineurs, la sanction est une peine privative de liberté de cinq ans au plus ou une peine pécuniaire.

5 Quiconque consomme ou, pour sa propre consommation, fabrique, importe, prend en dépôt, acquiert, obtient par voie électronique ou d'une autre manière ou possède des objets ou représentations visés à l'al. 1, ayant comme contenu des actes d'ordre sexuel avec des animaux, des actes de violence entre adultes ou des actes d'ordre sexuel non effectifs avec des mineurs, est puni d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire. Si les objets ou représentations ont pour contenu des actes d'ordre sexuel effectifs avec des mineurs, la sanction est une peine privative de liberté de trois ans au plus ou une peine pécuniaire.

6 En cas d'infraction au sens des al. 4 et 5, les objets sont confisqués.

7 Si l'auteur agit dans un dessein d'enrichissement, le juge prononce une peine pécuniaire en plus de la peine privative de liberté.

8 N'est pas punissable le mineur âgé de 16 ans ou plus qui produit, possède ou consomme, avec le consentement d'un autre mineur âgé de 16 ans ou plus, des objets ou des représentations au sens de l'al. 1 qui les impliquent.

9 Les objets et représentations visés aux al. 1 à 5 qui présentent une valeur culturelle ou scientifique digne de protection ne sont pas de nature pornographique.

Avant de détailler la disposition, certaines délimitations et précisions s'avèrent opportunes. Tout d'abord, il est pertinent de distinguer la pornographie légale (ou douce) de la pornographie illicite (interdite ou dure). Tandis que la pornographie dure est illégale dans toute situation, la pornographie

douce est rendue illicite lorsqu'elle est exposée à un mineur de moins de 16 ans ou en public, ou lorsqu'elle est offerte à une personne sans y avoir été invité. Par pornographie interdite, l'on entend les supports ayant comme contenu des actes d'ordre sexuel avec des animaux, des actes de violence entre adultes[27], et les actes d'ordre sexuel – effectifs et non effectifs – avec des mineurs (art. 197 al. 4 et 5 CP).

D'autre part, selon l'alinéa 1, le support pornographique peut consister en « des écrits, enregistrements sonores ou visuels, images ou autres objets pornographiques ou des représentations pornographiques ». La jurisprudence du Tribunal fédéral précise que la diffusion par le biais d'un téléphone ou d'Internet est couverte par la disposition[28].

Enfin, au sens du droit suisse, la mise en scène pornographique d'une personne, qu'elle soit réelle ou non (dans le cas d'un trucage) est considérée comme étant un contenu pornographique[29].

L'art. 197 CP vise notamment à protéger le développement sexuel paisible des jeunes et la jeunesse de manière générale. Ainsi, nous nous intéressons plus en détails à comment les mineurs sont protégés par cette norme légale en exposant quels sont les comportements criminalisés et quelles sont les peines menaces encourues. Le Tableau 4, ci-dessous, synthétise les comportements prohibés. D'une part, la loi interdit la fabrication, la possession, la diffusion et la consommation de matériel ayant comme contenu des actes d'ordre sexuel – effectifs ou non effectifs – avec des mineurs (al. 4 et 5). D'autre part, elle criminalise également le fait de mettre à disposition du matériel pornographique à un mineur de moins 16 ans (al. 1) ou encore de recruter un mineur en vue de l'inciter à participer à une représentation pornographique (al. 3)[30].

[27] Dans le cadre de l'actuelle révision du droit pénal, la Commission des affaires juridiques du Conseil des Etats propose de supprimer les actes de violence entre adultes aux alinéas 4 et 5 de l'art. 197 CP. Ces représentations seront réprimandées sous les alinéas 1 ou 2, ou encore sous l'art. 135 CP (représentation de la violence) (Commission des affaires juridiques du Conseil des Etats, 2022, p. 51).
[28] ATF 131 IV 64, c. 10.1.2.
[29] Cambi Favre-Bulle (2017).
[30] La disposition suisse va même au-delà de l'art. 9 de la Convention de Budapest portant sur la pornographie enfantine, et satisfait aux art. 20 et 21 de la Convention de Lanzarote concernant la pornographie enfantine et la participation d'un enfant à des spectacles pornographiques.

Tab. 4 – Comportements criminalisés en matière de pédopornographie selon l'art. 197 CP

Comportement criminalisé	Peines menace encourues
Mise à disposition ou diffusion de contenu ou représentations pornographiques à un mineur de moins de 16 ans (alinéa 1)	Peine privative de liberté de trois ans au plus OU peine pécuniaire
Recrutement en vue de ou incitation d'un mineur en vue de participer à une représentation pornographique (alinéa 3)	Peine privative de liberté de trois ans au plus OU peine pécuniaire
Fabrication, possession, mise à disposition d'objets ou représentations ayant comme contenu des actes d'ordre sexuel effectifs ou non effectifs avec des mineurs (alinéa 4)	Actes d'ordre sexuel *non effectifs* : peine privative de liberté de trois ans au plus OU peine pécuniaire Actes d'ordre sexuel *effectifs* : peine privative de liberté de cinq ans au plus OU peine pécuniaire
Consommation, et fabrication et possession pour sa propre consommation, d'objets ou de représentations ayant comme contenu des actes d'ordre sexuel effectifs ou non effectifs avec des mineurs (alinéa 5)	Actes d'ordre sexuel *non effectifs* : peine privative de liberté d'un an au plus OU peine pécuniaire Actes d'ordre sexuel *effectifs* : peine privative de liberté de trois ans au plus OU peine pécuniaire

Quant à la peine encourue, il peut s'agir d'une peine pécuniaire ou d'une peine privative de liberté allant jusqu'à, respectivement, un an, trois ans et cinq ans selon l'acte commis[31]. La peine menace de privation de liberté la moins élevée (1 an) concerne la consommation d'objets ou de représentations ayant comme contenu des actes d'ordre sexuel non effectifs avec des mineurs. Tandis que la peine menace la plus élevée (5 ans) se rapporte à la fabrication, la possession, et la mise à disposition d'objets ou représentations ayant comme contenu des actes d'ordre sexuel effectifs avec des mineurs.

2.2.2 Cyber grooming ou pédopiégeage

Plusieurs appellations francophones sont utilisées pour faire référence au cyber grooming, comme le pédopiégeage, la corruption d'enfants, la sollicitation d'enfants à des fins sexuelles, ou encore le leurre d'enfants. Outre les différences de terminologie, des variations entre pays, voire entre auteurs, sont observées en lien avec la définition qui est donnée à ce phénomène, de même qu'en relation avec le champ d'application des législations.

La principale distinction est celle de la conception du cyber grooming, qui peut être entendue au sens large ou au sens strict. La Convention de Lanzarote définit la sollicitation d'enfants à des fins sexuelles comme « le fait pour un adulte de proposer intentionnellement, par le biais des technologies de communication et d'information, une rencontre à un enfant n'ayant pas atteint l'âge fixé en application de l'article 18, paragraphe 2, dans le but de commettre à son encontre une infraction établie conformément aux articles 18, paragraphe 1.a, ou 20, paragraphe 1.a, lorsque cette proposition a été suivie d'actes matériels conduisant à ladite rencontre »[32]. Les deux articles cités font référence aux activités sexuelles et à la production de pornographie enfantine. La perspective adoptée par la Convention de Lanzarote peut dès lors être considéré comme étant la définition du cyber grooming au sens strict[33]. Au contraire, le cyber grooming au sens large prend en considération les étapes

[31] En comparant les peines menaces maximales, en termes de privation de liberté, de 22 pays à travers le monde, Burkhardt, da Silva, et Caneppele (2020) relèvent que celles-ci varient largement entre 2 et 20 ans.
[32] Précisions que la Suisse a émis une réserve concernant l'art. 24 de la Convention de Lanzarote, qui demande aux Parties d'incriminer la complicité et la tentative. Dans le contexte suisse, cela reviendrait à punir la tentative de la tentative.
[33] Meyer (2020).

antérieures à la rencontre, à savoir le processus de mise en confiance, voire de manipulation psychologique, mis en place par l'auteur[34], ainsi que les actes de harcèlement sexuel, « sans que ces agissements visent nécessairement une rencontre réelle ou remplissent les conditions d'un abus sexuel (ou de la tentative d'un tel abus) avec des enfants ou celles de la production (ou d'une tentative de production) de pornographie enfantine »[35,36].

Bien qu'aucune norme criminalise expressément le cyber grooming, le droit en vigueur criminalise le cyber grooming au sens étroit notamment au travers de l'art. 187 CP ci-dessous ou de l'art. 197 al. 4 CP en lien avec l'art. 22 CP.

Article 187 – Actes d'ordre sexuel avec des enfants

1 Celui qui aura commis un acte d'ordre sexuel sur un enfant de moins de 16 ans,

celui qui aura entraîné un enfant de cet âge à commettre un acte d'ordre sexuel,

celui qui aura mêlé un enfant de cet âge à un acte d'ordre sexuel,

sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.

2 L'acte n'est pas punissable si la différence d'âge entre les participants ne dépasse pas trois ans.

3 Si, au moment de l'acte ou du premier acte commis, l'auteur avait moins de 20 ans et en cas de circonstances particulières ou si la victime a contracté mariage ou conclu un partenariat enregistré avec l'auteur, l'autorité compétente peut renoncer à le poursuivre, à le renvoyer devant le tribunal ou à lui infliger une peine.

4 La peine sera une peine privative de liberté de trois ans au plus ou une peine pécuniaire si l'auteur a agi en admettant par erreur que sa victime était âgée de 16 ans au moins alors qu'en usant des précautions voulues il aurait pu éviter l'erreur.

Les biens juridiques protégés par l'art. 187 CP est le développement sexuel paisible des enfants ainsi que l'incapacité de consentir valablement à un acte d'ordre sexuel[37]. Par acte d'ordre sexuel, l'on entend « une activité corporelle sur soi-même ou sur autrui qui tend à l'excitation ou à la jouissance sexuelle de l'un des participants au moins »[38]. L'acte doit posséder « pour un observateur neutre et extérieur, une connotation sexuelle manifeste »[39]. Plus précisément, trois comportements sont punissables : le fait de commettre un acte d'ordre sexuel sur un enfant de moins de 16 ans, le fait de l'entraîner à commettre un tel acte – sur son propre corps, sur un tiers ou sur un animal –, ou finalement le fait de le mêler à un tel acte. Pour les deux dernières alternatives (entraîner et mêler), un contact physique entre l'auteur et l'enfant n'est pas requis. De même que l'auteur ne doit pas obligatoirement se trouver au même endroit que la victime, l'utilisation de messagerie instantanée ou de webcam est admis[40].

[34] Meyer (2020).
[35] Commission des affaires juridiques du Conseil des États (2022, p. 67).
[36] Pour plus d'informations sur la distinction entre cyber grooming au sens strict et cyber grooming au sens large, ainsi qu'une analyse juridique du droit suisse et des lacunes en matière de sollicitation d'enfants à des fins sexuelles, nous renvoyons le lecteur au travail de Meyer (2020).
[37] Zermatten (2017).
[38] Corboz (2010, p. 785); Zermatten (2017, p. 920).
[39] Zermatten (2017, p. 921) ; ATF 125 IV 58 c. 3b.
[40] Zermatten (2017).

Selon la jurisprudence du Tribunal fédéral, lorsqu'une personne propose à un mineur de moins de 16 ans une rencontre sexuelle et se rend au rendez-vous avec l'intention de commettre un acte d'ordre sexuel, la tentative inachevée d'actes d'ordre sexuel sur un enfant au sens de l'art. 187 ch. 1 CP (en relation avec l'art. 22 CP) peut être retenue[41], pour autant que l'abus ne soit pas réalisé. Cependant, pour que les éléments constitutifs soient remplis, la jurisprudence exige un lien spatial et temporel étroit avec la réalisation de l'infraction[42]. En d'autres termes, l'auteur doit accomplir « un acte qui représente, dans son esprit, la démarche ultime et décisive vers la réalisation de l'infraction, celle après laquelle il n'y aura en principe plus de retour en arrière, sauf apparition ou découverte de circonstances extérieures compliquant trop ou rendant impossible la poursuite de l'entreprise »[43]. En ce sens, le fait de proposer une rencontre à des fins sexuelles[44] ou même d'acheter un billet de transport public n'est pas suffisant.

Par analogie, si un adulte propose à un enfant une rencontre en vue de produire un objet ou une représentation ayant comme contenu des actes d'ordre sexuel avec l'enfant, une tentative de production de matériel pornographique est applicable (art. 197 al. 4 CP, en relation avec art. 22 CP) « si la rencontre a lieu et qu'elle constitue la dernière étape décisive avant la réalisation de l'infraction »[45].

Au niveau de la peine menace, le prononcé d'une tentative implique une atténuation de la peine. Toutefois, les actes précédant la rencontre pourront être considérés dans l'examen de l'intention et influer sur la quotité de la peine. Enfin, une mesure thérapeutique au sens des art. 63 et 59 CP peut être prononcée si une un trouble psychiatrique, par exemple de pédophilie, est diagnostiqué[46].

Depuis le début des années 2000, plusieurs initiatives politiques ont été lancées afin de criminaliser les abus commis en ligne à l'encontre des mineurs[47]. Dans le cadre de la révision actuelle du droit pénal en matière sexuelle, l'opportunité de créer une disposition spécifique pour le pédopiégeage a été discutée. Bien qu'une nette majorité des participants à la consultation étaient en faveur d'une telle disposition, la Commission des affaires juridique du Conseil des Etats (CAJ-E) n'a pas souhaité introduire une telle infraction en raison que le pédopiégeage au sens strict est déjà punissable par le

[41] ATF 131 IV 100, c. 8.2.
[42] ATF 131 IV 100, c. 8.1.
[43] ATF 131 IV 100, c. 7.2.1.
[44] En droit français, selon l'art. 227-22-1 Code pénal, la simple proposition sexuelle à un mineur est punissable. « Le fait pour un majeur de faire des propositions sexuelles à un mineur de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Ces peines sont portées à cinq ans d'emprisonnement et 75 000 euros d'amende lorsque les propositions ont été suivies d'une rencontre ».
[45] Commission des affaires juridiques du Conseil des États (2022, p. 68).
[46] Zermatten (2017).
[47] Dans son analyse, Meyer (2020) répertorie plusieurs initiatives portant sur la thématique : Motion 07.3449 « Rendre punissable les abus virtuels commis sur des enfants par le biais d'Internet » déposée le 21 juin 2007 par Viola Amherd ; Motion 11.4002 « Eriger en infraction pénale la sollicitation d'enfants à des fins sexuelles » déposée le 30 septembre 2011 par Barbara Schmid-Federer ; l'initiative parlementaire 13.442 « Grooming avec des mineurs » déposée le 15 août 2013 par la Commission des Affaires juridiques du Conseil national ; Initiative parlementaire 18.434 « Punir enfin le pédopiégeage en ligne » déposée le 14 juin 2018 par Viola Amherd ; Interpellation 18.4121 « De plus en plus d'enfants sont victimes de harcèlement sexuel sur Internet. Que fait le Conseil fédéral ? » déposée le 29 novembre 2018 par Yvonne Feri.

droit en vigueur[48]. Dans son avis du 13 avril 2022[49], le Conseil fédéral s'est prononcé en faveur du projet de la CAJ-E[50].

En revanche, au regard du droit suisse, avant même de se rendre à un rendez-vous à des fins sexuelles avec un mineur, certains actes propices pour le pédopiégeage en ligne peuvent être réprimés par d'autres dispositions légales (cyber grooming au sens large), notamment[51,52] :

- Art. 197 al. 1 CP : mise à disposition au mineur de textes ou d'images pornographiques.
- Art. 187 ch. 1 CP : entraîner le mineur de moins de 16 ans à commettre des actes d'ordre sexuel sur son propre corps.
- Art. 187 ch. 1 CP : mêler un mineur de moins de 16 ans à un acte d'ordre sexuel. Le fait d'« entendre des bruits ou des paroles d'actes sexuels » suffit pour matérialiser l'infraction, de même que de voir ledit acte via une webcam[53].
- Art. 198 al. 2 CP : le fait d'importuner une personne par des paroles grossières.

Nous revenons brièvement sur l'art. 198 CP, ci-dessous, portant sur les désagréments causés par la confrontation à un acte d'ordre sexuel, qui peut potentiellement trouver application.

Article 198 – Désagréments causés par la confrontation à un acte d'ordre sexuel

Celui qui aura causé du scandale en se livrant à un acte d'ordre sexuel en présence d'une personne qui y aura été inopinément confrontée,

celui qui aura importuné une personne par des attouchements d'ordre sexuel ou par des paroles grossières, sera, sur plainte, puni d'une amende.

La portée relativement restreinte de cette disposition a été débattue dans le cadre de la révision du droit pénal. *In fine*, la CAJ-E a retenu la proposition d'élargir le champ d'application de la disposition à l'écriture et à l'image de contenu sexuel[54]. De plus, alors que la lettre de la loi requière plus d'une parole, le singulier est retenu dans la nouvelle formulation.

[48] Selon la CAJ-E, « une nouvelle disposition pénale distincte n'élargirait que peu le champ d'application actuel, de sorte que son avantage pratique est douteux. L'ajout d'une telle disposition dans la loi n'aurait de ce fait qu'une valeur symbolique » (Commission des affaires juridiques du Conseil des États, 2022, p. 69).
[49] Conseil fédéral (2022).
[50] A l'exception de l'introduction de l'art. 197a P-CP criminalisant la pornodivulgation (Conseil fédéral, 2022, p. 3).
[51] Commission des affaires juridiques du Conseil des États (2022).
[52] La Commission des affaires juridiques du Conseil des Etats (2022) mentionne aussi la possible application des art. 179^{quater} CP (violation du domaine secret ou du domaine privé au moyen d'un appareil de prise de vues), 180 CP (menaces), 181 CP (contrainte).
[53] Meyer (2020, p. 10).
[54] Commission des affaires juridiques du Conseil des États (2022).

2.2.3 Sextorsion

La sextorsion peut se manifester sous plusieurs scénarios, faisant appel à des normes pénales distinctes. Nous illustrons dans cette section les trois scénarios les plus courants.

Scénario 1 : l'auteur menace de diffuser du matériel à contenu sexuel mettant en scène une victime mineure, et exige de la victime qu'elle paye une somme d'argent en échange de la non-diffusion dudit matériel. Dans ce cas d'espèce, l'art 156 CP, ci-dessous, réprimant l'extorsion peut trouver application. D'une part, la victime doit être contrainte à effectuer un acte de disposition préjudiciable à ses intérêts pécuniaires (en cédant une somme d'argent par exemple), et d'autre part, l'auteur doit poursuivre un enrichissement illégitime qui est compris ici sous l'angle économique, à savoir un gain ou une non-dépense.

Article 156 – Extorsion et chantage

1 Celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura déterminé une personne à des actes préjudiciables à ses intérêts pécuniaires ou à ceux d'un tiers, en usant de violence ou en la menaçant d'un dommage sérieux, sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.

2 Si l'auteur fait métier de l'extorsion ou s'il a poursuivi à réitérées reprises ses agissements contre la victime, la peine sera une peine privative de liberté de un à dix ans.

3 Si l'auteur a exercé des violences sur une personne ou s'il l'a menacée d'un danger imminent pour la vie ou l'intégrité corporelle, la peine sera celle prévue à l'art. 140.

4 Si l'auteur a menacé de mettre en danger la vie ou l'intégrité corporelle d'un grand nombre de personnes ou de causer de graves dommages à des choses d'un intérêt public important, la peine sera une peine privative de liberté d'un an au moins.

Scénario 2 : l'auteur menace de diffuser du matériel à contenu sexuel mettant en scène une victime mineure, et exige de la victime qu'elle fournisse d'autres images en échange de la non-diffusion dudit matériel. Dans le cas d'espèce, l'élément constitutif de l'enrichissement illégitime n'est pas présent, rendant ainsi l'application de l'art. 156 CP impossible. En revanche, la demande d'images supplémentaires peut remplir les critères d'application de la contrainte (art. 181 CP) et/ou de la menace (art. 180 CP).

Article 181 – Contrainte

Celui qui, en usant de violence envers une personne ou en la menaçant d'un dommage sérieux, ou en l'entravant de quelque autre manière dans sa liberté d'action, l'aura obligée à faire, à ne pas faire ou à laisser faire un acte sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

Article 180 – Menaces

1 Celui qui, par une menace grave, aura alarmé ou effrayé une personne sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

2 La poursuite aura lieu d'office :

a. si l'auteur est le conjoint de la victime et que la menace a été commise durant le mariage ou dans l'année qui a suivi le divorce ;

a^{bis}. si l'auteur est le partenaire de la victime et que la menace a été commise durant le partenariat enregistré ou dans l'année qui a suivi sa dissolution judiciaire ;

b. si l'auteur est le partenaire hétérosexuel ou homosexuel de la victime pour autant qu'ils fassent ménage commun pour une durée indéterminée et que la menace ait été commise durant cette période ou dans l'année qui a suivi la séparation.

Scénario 3 : l'auteur menace de diffuser plusieurs matériels à contenu sexuel mettant en scène une victime mineure, et exige de la victime qu'elle fournisse d'autres images en échange de la non-diffusion dudit matériel ou qu'elle paye une somme d'argent. Pour rendre crédible sa menace, l'auteur diffuse une première image. En plus des dispositions légales exposées dans les scénarios précédents, la diffusion d'une première image peut constituer une atteinte à l'honneur au sens de l'art. 173 ch. 1 CP (diffamation), ci-dessous, ainsi que la diffusion d'une image à contenu pornographique au sens de l'art. 197 al. 1 ou al. 4 CP (selon la nature de l'image). Précisions que pour remplir les éléments constitutifs de la diffamation, l'image doit avoir été portée à la connaissance d'un tiers.

Article 173 – Diffamation

1 Celui qui, en s'adressant à un tiers, aura accusé une personne ou jeté sur elle le soupçon de tenir une conduite contraire à l'honneur, ou de tout autre fait propre à porter atteinte à sa considération, celui qui aura propagé une telle accusation ou un tel soupçon, sera, sur plainte, puni d'une peine pécuniaire.

2 L'inculpé n'encourra aucune peine s'il prouve que les allégations qu'il a articulées ou propagées sont conformes à la vérité ou qu'il avait des raisons sérieuses de les tenir de bonne foi pour vraies.

3 L'inculpé ne sera pas admis à faire ces preuves et il sera punissable si ses allégations ont été articulées ou propagées sans égard à l'intérêt public ou sans autre motif suffisant, principalement dans le dessein de dire du mal d'autrui, notamment lorsqu'elles ont trait à la vie privée ou à la vie de famille.

[…]

D'autres scénarios sont imaginables entraînant l'application d'infractions périphériques telles que la soustraction de données (art. 143 CP), l'accès indu à un système informatique (art. 143bis CP).

2.2.4 Live-streaming

Le live-streaming consiste en la diffusion en direct d'actes d'ordre sexuel effectués par un mineur sur lui-même ou par une personne tierce sur le mineur. En l'espèce, ce comportement correspond aux actes d'ordre sexuel réprimés à l'art. 187 CP[55] (*supra*, ch. 2.2.2). Bien qu'il puisse également s'agir d'une incitation à participer à une représentation pornographique au sens de l'art. 197 al. 3 CP, l'art. 187 CP prime sur l'art. 197 CP dès lors qu'il y a un contact physique, et pour autant que la victime soit âgée de moins de 16 ans. Comme relevé précédemment, le contact physique n'est pas forcément entre l'auteur et la victime. Un acte d'ordre sexuel commis par la victime sur elle-même, par la victime sur un tiers, ou par l'auteur sur lui-même remplit les critères d'application de l'art. 187 ch. 1 CP[56]. De plus, nous avions relevé également que la victime et l'auteur ne doivent pas forcément se trouver au même endroit, des actes d'ordre sexuel via webcam étant admissibles[57].

En outre, en présence d'une contrepartie financière ou de la promesse d'une telle contrepartie, l'art. 196 CP, ci-dessous, s'applique conjointement à l'art. 187 CP.

> **Article 196 – Actes d'ordre sexuel avec des mineurs contre rémunération**
>
> Quiconque, contre une rémunération ou une promesse de rémunération, commet un acte d'ordre sexuel avec un mineur ou l'entraîne à commettre un tel acte est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

D'autre part, en matière de live-streaming, il arrive qu'un auteur, par caméra interposée, paye un show où une tierce personne fait « subir un acte d'ordre sexuel à un mineur afin de réaliser son propre fantasme »[58]. Dans ce scénario, la participation de l'auteur peut être considérée comme de l'instigation ou de la commission médiate (auteur médiat).

Enfin, dans l'hypothèse où la victime a au moins 16 ans et moins de 18 ans, et qu'une contrepartie financière ou matérielle quantifiable[59] – ou une promesse d'une telle contrepartie – est donnée, seule l'art. 196 CP s'applique.

2.2.5 Autres sanctions possibles

Lors d'une condamnation pour certains délits ou crimes, d'autres mesures peuvent être prononcées en complément par le juge.

a) Expulsion du territoire

Selon l'art. 66a CP, un étranger condamné pour acte d'ordre sexuel sur un mineur de moins de 16 ans (art. 187 ch. 1 CP) ou pour pornographie dure (art. 197 al. 4, 2e phrase CP) peut se voir expulser du territoire suisse pour une durée de cinq à quinze ans.

[55] En matière de live-streaming, d'autres infractions contre l'intégrité sexuelle pourraient être retenues dépendant des faits survenus (art. 188 à 193 CP).
[56] Zermatten (2017).
[57] Zermatten (2017).
[58] Zermatten (2017, p. 943).
[59] Pedrazzini Rizzi (2017).

b) Interdiction d'exercer une activité professionnelle

Lors d'une condamnation pour un délit ou un crime contre un mineur, notamment en matière d'actes d'ordre sexuel ou de pornographie (une seule image suffit), le juge peut prononcer une interdiction d'exercer une activité professionnelle impliquant un contact régulier avec des mineurs pour une durée d'un à dix ans (art. 67 al. 2), voire à vie (al. 2bis et 3). Durant la période d'interdiction, une assistance de probation peut être ordonnée (al. 6).

c) Confiscation d'objet

Le juge peut prononcer une confiscation des objets ayant servi à commettre une infraction ou étant le produit d'une infraction, « si ces objets compromettent la sécurité des personnes, la morale ou l'ordre public » (art. 69 al. 1 CP). Or, la pornographie dure – au sens des art. 197 al. 4 et 5 –, compromet « la morale et la sécurité publique aussitôt qu'un risque de diffusion existe »[60]. Ainsi, les équipements utilisés pour la réalisation de matériel pornographique (instruments du délit), ainsi que le matériel réalisé et son support (vidéo, images, ordinateur, téléphone portable, etc. ; produit du délit) peuvent être confisqués[61]. Outre la confiscation au sens de l'art. 69 CP, l'art. 197 al. 6 prévoit automatiquement la confiscation des objets de pornographie dure.

d) Mesures thérapeutiques ou de sûreté

Selon l'art. 56 CP, une mesure doit être ordonnée si « une peine seule ne peut écarter le danger que l'auteur commette d'autres infractions » (al. 1, let. a), « si l'auteur a besoin d'un traitement ou que la sécurité publique l'exige » (al. 1, let. b), et « si les conditions prévues aux art. 59 à 61, 63 ou 64 sont remplies » (al. 1, let. c). Par exemple, si un trouble psychique de pédophilie est diagnostiqué, une mesure thérapeutique ou sécuritaire peut être prononcée en sus de la peine privative de liberté (art. 59, 63 ou 64 CP)[62].

2.3 Compétences et réseau de soutien en matière d'investigation et de poursuite pénale dans le domaine de la cybercriminalité

Dans cette section, nous décrivons brièvement la répartition des compétences entre la Confédération et les cantons. Ensuite, nous mentionnons les réseaux de coordination et d'appui existants en matière d'investigation et de poursuite pénale.

2.3.1 Répartition des compétences entre les cantons et la Confédération

Le fédéralisme qui caractérise la Suisse implique une répartition des compétences entre la Confédération et les 26 cantons qui la composent. Conformément à la Constitution suisse et au code de procédure pénale, la compétence en matière de police et de poursuite pénale est conférée aux cantons (polices cantonales, ministères publics cantonaux). Ils demeurent toutefois certaines exceptions soumises à la juridiction fédérale (art. 23 et 24 CPP) , notamment à travers la police fédérale (fedpol) et le Ministère public de la Confédération (MPC). Au niveau police, il s'agit essentiellement

[60] Cambi Favre-Bulle (2017, p. 1040).
[61] Hirsig-Vouilloz (2021); Zermatten (2017).
[62] Zermatten (2017).

des crimes relevant de la grande criminalité et de la coopération internationale. En matière de poursuites pénales, sont de la compétence du MPC les délits en série intercantonaux ou internationaux, ainsi que la criminalité organisée.

L'expansion de la criminalité informatique, et par conséquent des réponses préventives et répressives, a nécessité que la Confédération et les cantons joignent leurs forces et leurs ressources. En termes de lutte contre la pédocriminalité (en ligne et hors ligne), bien que la compétence soit conférée aux cantons, fedpol assume les tâches d'office central en vertu de la Loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États (LOC)[63]. En d'autres termes, fedpol détient un rôle relevant essentiellement de la coordination supra cantonale et internationale. Fedpol est ainsi le point de contact pour la coopération internationale, incluant les collaborations avec les organisations telles que Interpol et Europol, et pour l'organisation américaine National Center for Missing & Exploited Children (NCMEC) qui envoie des annonces, provenant notamment de fournisseurs de services de télécommunication américains qui ont un lien réel ou supposé avec la Suisse[64]. Fedpol effectue une première analyse, d'une part, quant à la nature illicite en regard du droit pénal suisse et, d'autre part, sur l'identification de l'expéditeur du contenu. Le dossier est ensuite transmis au canton concerné en vue d'investigations ultérieures et/ou d'ouverture d'une procédure pénale. À titre d'exemple, en 2020, fedpol a reçu 7852 annonces de soupçons de matériel pédopornographique de la part de NCMEC, pour lesquelles 1166 rapports ont été transmis aux cantons (représentant ainsi 14,8% des annonces de soupçons).

Tab. 5 – Nombre d'annonces de soupçons envoyées par NCMEC à fedpol, et nombre de rapports transmis par fedpol aux cantons

	Annonces de soupçons	Rapports transmis aux cantons	
	Nombre	Nombre	% des annonces de soupçons
2021	7176	1399	19,5%
2020	7852	1166	14,8%
2019	8028	693	8,6%
2018	9167	612	6.7%
2017	5404	428	7,9%
2016	2994	261	8,7%

Source : Rapports fedpol en chiffres 2020 et 2021. Lutte contre la pédocriminalité[65].

Fedpol gère également les bases de données nationales et internationales. Par exemple, l'ICSE (Internet Child Sexual Exploitation) est une base de données d'images et de vidéos créée par Interpol et reliée aux polices de 64 pays à travers le monde[66]. Cet outil de renseignements et d'enquête sert notamment à identifier les victimes, à déterminer si un matériel à contenu illicite est connu ou pas, et à échanger des informations entre policiers via un forum de discussion.

[63] RS 360. Entrée en vigueur le 7 octobre 1994.
[64] Conférence des directrices et directeurs des départements cantonaux de justice et police (2020).
[65] https://2020.fedpol.report/de/fedpol-in-zahlen/kampf-gegen-paedokriminalitaet ; https://fedpol.report/fr/fedpol-en-chiffres/lutte-contre-la-pedocriminalite
[66] https://www.interpol.int/fr/Infractions/Pedocriminalite/Base-de-donnees-internationale-sur-l-exploitation-sexuelle-des-enfants

2.3.2 Réseaux de soutien et d'appui

La compétence étant répartie entre les 26 cantons, un travail de coordination intra cantonal est primordial. Plusieurs réseaux ou centre de compétences sont opérationnels en matière de cybercriminalité à l'échelle nationale ou régionale.

a) Au niveau national

Nous relevons trois réseaux principaux en matière de cybercriminalité : le Centre national pour la cybersécurité (NCSC)[67], le réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK), et la plateforme de dialogue stratégique au niveau de la procédure pénale (Cyberboard).

En matière de cyber pédocriminalité, nous nous intéressons plus particulièrement au réseau NEDIK qui a été créé en 2018 par la Conférence des commandantes et commandants des polices cantonales suisses. Il a pour objectif de concentrer les ressources spécialisées et renforcer la coordination policière entre les cantons – et entre la Confédération et les cantons –, en matière de cybercriminalité, y compris pour la pédocriminalité. En revanche, ce réseau n'a pas de compétence en matière d'enquête[68]. Une rencontre mensuelle est organisée afin d'établir un état de situation de la cybercriminalité en Suisse.

Sous l'angle de la poursuite pénale, la stratégie nationale de lutte contre les cyberrisques[69] a créé, en mai 2018, le Cyberboard, à savoir une plateforme de dialogue stratégique regroupant notamment le MPC, fedpol et des autorités judiciaires et policières cantonales. Le Cyberboard est structuré en quatre unités, parmi lesquelles l'unité opérationnelle cyber-CASE. Une rencontre mensuelle a lieu afin d'harmoniser la poursuite pénale en matière de cybercriminalité[70].

b) Au niveau régional

Afin de mutualiser le savoir, les ressources et l'infrastructure, certaines activités policières sont centralisées auprès d'une police cantonale. Ainsi, la coordination des affaires de téléchargements Peer-to-Peer est gérée par la police cantonale de Berne pour l'ensemble de la Suisse, et la gestion du savoir est encadrée par la police cantonale de Saint-Gall.

D'autre part, une Centre régional de lutte contre la cybercriminalité (RC3) a été crée par le concordat RBT pour la Romandie, le Tessin et le canton de Berne, qui concentre ses activités principalement sur trois axes : les investigations avancées sur les supports numériques, les enquêtes sur les ransomware, la lutte contre la pédopornographie. En matière de pédopornographie, quatre pôles de compétence sont identifiés : les annonces NCMEC transmises par fedpol, le monitoring de téléchargements Peer-to-

[67] Selon une décision de principe prise par le Conseil fédéral en date du 18 mai 2022, le NCSC deviendra prochainement un office fédéral à part entière (Conseil fédéral & Secrétariat général DFF, 2022).
[68] Schwegler (2022a).
[69] Le Département fédéral de la défense, de la protection de la population et des sports (DDPS) a élaboré une stratégie nationale de protection contre les cyberrisques. La première était constituée de 16 actions à mettre en œuvre pour les années 2012 à 2017. Le 18 avril 2018, le Conseil fédéral a approuvé la seconde stratégie qui prévoit les travaux pour la période 2018-2022. Afin d'atteindre les sept objectifs stratégiques déterminés, 29 mesures ont été formulées, réparties en 10 champs d'action (Conseil fédéral, 2018). Les mesures du champ d'action « Poursuite pénale » concerne, entre autres choses, l'élaboration d'un tableau permettant d'avoir une vue d'ensemble de la situation en matière de cybercriminalité, que ce soit sous l'angle des infractions enregistrées par la police que des affaires judiciaires en cours, incluant dès lors les actes de pédocriminalité en ligne.
[70] Conseil fédéral (2020b).

Peer, les recherches préventives secrètes sur les chats, et l'achat de matériel pédopornographique à l'aide de cryptomonnaie.

Au niveau régional, nous pouvons également citer la plateforme d'information de la criminalité sérielle en ligne PICSEL, qui est un outil de renseignements permettant de détecter des séries d'infractions. Elle est administrée par la Police cantonale genevoise et accessible à toutes les polices du concordat RBT, fedpol et le canton d'Argovie[71]. Un projet d'étendre l'utilisation de PICSEL à l'échelle nationale est en cours[72].

[71] Röösli (2022).
[72] Cette expansion requiert divers travaux en amont dont la création d'une base juridique et l'exploitation d'une nouvelle plateforme technique (Röösli, 2022).

3. Méthodologie

Le présent chapitre décrit les méthodes utilisées afin de récolter les données et renseignements nécessaires pour accomplir ce mandat (Tab. 6). De manière générale, les résultats se fondent sur quatre sources de données : la littérature scientifique, la littérature grise, les réponses à un questionnaire, les réponses issues d'entretiens.

Tab. 6 – Aperçu des questions de recherche et des sources analysées

Questions de recherche	**Type de question***	**Données analysées**			
		Littérature scientifique	Questionnaire	Littérature grise	Entretiens avec des experts
1.1a. Types de plateformes et de chats, types d'activités.	D	●			●
1.1b. Caractéristiques des victimes et des agresseurs.	D	●			●
1.2 Mesures existantes en Suisse.	D		●	●	○
1.3 Acteurs et réseaux principaux proposant des mesures en Suisse.	D		●	●	○
1.4 Destinataires des mesures.	D		○	●	○
2.1. Possibilités et limites des mesures.	E			○	●
2.2. Efficacité des mesures et bonnes pratiques.	E			○	●
2.3. Lacunes des mesures.	E			○	●
2.4. Recommandations pour la Suisse.	E	○	○	●	●

** Types de question : Descriptive (D) ou Evaluative (E)*

Légende : ● *Les données ont apportées une contribution significative à la réponse aux questions ;*
○ *Les données ont apportées une contribution supplémentaire à la réponse aux questions.*

3.1 Analyse documentaire sur les quatre phénomènes à investiguer

Afin de répondre aux buts et objectifs de la recherche, nous avons procédé à une évaluation rapide des données probantes (*Rapid Evidence Assessment*).

Ainsi, une revue de littérature sur les études récentes a été réalisée pour chacun de ces phénomènes : la production et la distribution de matériel pédopornographique via Internet, le cyber grooming, la sextorsion et le live-streaming d'actes d'ordre sexuel. Les revues de littérature sont basées sur les 100 premiers résultats des requêtes d'articles parus dans des revues scientifiques ainsi que des thèses de mémoire ou de doctorat, accessibles depuis le moteur de recherche Google Scholar et publiées depuis 2016 en anglais, français et allemand selon 12 combinaisons de mots-clés standardisées[73] (Annexe B). Pour être incluse dans la revue, la publication doit : a) avoir un titre ou un résumé pertinent ; b) traiter des caractéristiques des auteurs, des victimes ou du mode opératoire ; c) provenir d'Europe, d'Amérique du Nord ou d'Australie.

[73] Des recherches exploratoires de pertinence de mots-clés ont été menées avant de construire les requêtes de Google scholar. La pertinence des mots-clés a été évaluée selon les titres des résultats de recherche. Les combinaisons identifiées étaient : Phénomène recherché AND (auteur* OR victim* OR "modus operandi" OR "mode opératoire") ; Phénomène recherché AND (*Täter* OR Opfer* OR "Modus Operandi") ; Phénomène recherché AND (offender* OR victim* OR "modus operandi").

Pour les revues, les publications ont été répertoriées selon six catégories : 1) le titre de l'article ; 2) le nom de l'auteur avec l'année de publication ; 3) le(s) type(s) de phénomène(s) étudié(s) ; 4) la méthodologie utilisée pour mener la recherche ainsi que la source des données et la méthode d'analyse ; 5) la période temporelle investiguée dans le cadre de la recherche ; 6) les résultats obtenus[74].

Quelques chiffres sur l'analyse documentaire sur les phénomènes

105 manuscrits ont été recensés, dont 35 revues de littératures portant sur plusieurs études empiriques, et 70 manuscrits d'études empiriques originales[75].

La majorité des manuscrits se rapporte aux distributeurs et producteurs de pédopornographie (51%), suivie du cyber grooming (35%), de la sextorsion (9%) et du live-streaming de pédopornographie (5%).

Les manuscrits empiriques originaux proviennent majoritairement du monde anglosaxon (75%)[76].

Les données et la méthode de collecte de ces dernières varient en fonction du phénomène à l'étude[77] :

- *Production et distribution de pédopornographie* : entretiens et sondages menés auprès de populations judiciarisées.
- *Cyber grooming* : plutôt des retranscriptions de communications.
- *Sextorsion* : davantage de sondage de victimisation menés auprès de jeunes d'école secondaire.
- *Live-streaming de pédopornographie* : données policières.

3.2 Questionnaire en ligne sur les acteurs en Suisse, les initiatives et les collaborations

Une deuxième activité a recensé les acteurs actifs en Suisse, les mesures implémentées ou envisagées et les collaborations entre différents acteurs. Pour ce faire, l'équipe de recherche a élaboré un questionnaire en ligne construit sur la plateforme Limesurvey et accessible via un site Internet ouvert à ce propos.

Le questionnaire est composé de 19 questions (Annexe D) et aborde les initiatives que les acteurs ont organisé/coordonné ou auxquelles ils ont participé, les éventuelles mesures envisagées, les réseaux auxquels ils sont associés et leurs collaborations actuelles et futures avec d'autres organisations.

La majorité des invitations à participer au questionnaire a été envoyée entre novembre et décembre 2021 à sept catégories d'institution (Tab. 7). La collecte de données a été complétée en mars 2022 en adressant le questionnaire à une huitième catégorie (les tribunaux pénaux de première instance).

[74] La liste de toutes les études incluses peut être consultée dans l'annexe externe disponible en ligne, Section 1.
[75] Un manuscrit est une publication originale, tandis qu'une revue de littérature est un état des lieux d'un phénomène qui se fonde sur plusieurs manuscrits.
[76] En particulier des Etats Unis (27), de l'Australie (11), du Royaume Uni (9) et du Canada (8). La partie restante (25%) vient de l'Europe continentale et notamment depuis l'Espagne (8), l'Allemagne (3), la France (2), l'Autriche, la Finlande, l'Italie, le Portugal, la République Tchèque, la Suède et la Suisse (1). Au niveau de l'Europe continentale, les études sont ciblées en large majorité sur la production et distribution de matériel pédopornographique via Internet et le cyber grooming.
[77] Pour les recherches menées sur plusieurs dimensions d'intérêt, la source est insérée pour chaque phénomène analysé.

Tab. 7 – Catégories d'institution invitées à participer au questionnaire

Etablissements scolaires (écoles privées et publiques)	Départements gouvernementaux
Corps de police	Organisations de la société civile
Tribunaux des mineurs	Instituts de médecine sociale et préventive
Tribunaux pénaux de première instance	Entreprises privées

Au total, le questionnaire a été adressé à 447 différentes institutions et à 4 réseaux pour les écoles au sein des 26 cantons suisses susceptibles de mener des initiatives visant à protéger les enfants de délits commis en ligne.[78] En l'état, il est impossible de calculer un taux de réponse dès lors que les institutions contactées étaient encouragées à transmettre notre invitation à d'autres acteurs susceptibles d'être concernés par notre enquête (technique dite par boule de neige). En conséquence, le nombre exact d'institutions ayant eu connaissance de notre démarche demeure inconnue. Les critères d'exclusion suivants ont été appliqués afin de retenir les initiatives contribuant à répondre aux objectifs de l'étude :

- Les initiatives dont la description était trop vague pour en comprendre le format et le contenu.
- Les initiatives dont la description était concentrée sur l'identité numérique, la gestion des données personnelles, le cyberharcèlement, le sexting, l'éducation sexuelle.
- Les initiatives focalisées sur les auteurs mineurs.
- Les initiatives dont la portée se limitait à diffuser le matériel d'une autre institution ou d'une campagne à large échelle (par exemple, les corps de police ont largement diffusé les vidéos de la campagne nationale sur les cyber escroqueries).

[78] L'échantillonnage des institutions a été réalisé autour de huit catégories d'institutions : a) **ÉTABLISSEMENTS SCOLAIRES**. *Écoles publiques* : nous avons demandé à des conférences scolaires de diffuser l'invitation à participer au questionnaire : la Conférence latine des chefs d'établissements de la scolarité obligatoire (CLASECO), la Conférence des directrices et directeurs de gymnases suisses (CDGS), la *Verband Schulleiterinnen und Schulleiter Schweiz* (VSLCH), la Conférence suisse des directrices et directeurs d'écoles professionnelles (SDK-CSD). Concernant les écoles de culture générale, elles ont été contactées par le biais des adresses emails accessibles sur le site de la Conférence suisse des directeurs et directrices des écoles de culture générale. *Écoles privées* : contactées au travers de quatre registres renseignant sur les écoles privées en Suisse (https://www.swissprivateschoolregister.com ; https://www.suisse-romande.com/ecoles-privees.html ; https://www.privatschulen-schweiz.ch/fr/ ; https://www.swiss-schools.ch/) ; b) **POLICE** : les contacts ont été identifiés sur les sites Internet des 26 institutions policières cantonales en sélectionnant les adresses emails dédiées à la prévention et dans le cas échéant en contactant les adresses génériques. Trois polices municipales ont aussi été contactées, celle de Lugano, Lausanne et Zurich ; c) **TRIBUNAUX DES MINEURS** : contacts identifiés sur les sites Internet des autorités de justice en sélectionnant les adresses emails des tribunaux des mineurs, et le cas échéant des tribunaux cantonaux ou régionaux ; d) **TRIBUNAUX PÉNAUX DE PREMIÈRE INSTANCE** : contacts identifiés sur les sites Internet des autorités de justice ; e) **DÉPARTEMENTS GOUVERNEMENTAUX** : contactés à l'aide de la liste des membres de l'assemblée plénière de la Conférence pour la politique de l'enfance et de la jeunesse (CPEJ) et au travers des sites Internet des gouvernements cantonaux en contactant principalement les départements de la formation et de la culture. Sont également inclus dans cette catégorie des centres cantonaux d'assistance aux victimes et la Prévention Suisse de la Criminalité ; f) **ORGANISATIONS DE LA SOCIÉTÉ CIVILE** : organisations indépendantes de toute gouvernance étatique, à but non lucratif et œuvrant pour l'intérêt public. L'UNIL avait déjà mené une recherche d'organisations de la société civile active dans le domaine de la cybercriminalité pour les besoins du projet H2020 CC-DRIVER. ; g) **INSTITUTS DE MÉDECINE SOCIALE ET PRÉVENTIVE** (Berne, Vaud, Zurich); h) **ENTREPRISES PRIVÉES** : organisations dans le secteur d'activité des télécommunications. Contacts identifiés sur leur site Internet.

Quelques chiffres sur le questionnaire

134 institutions ont répondu au questionnaire.

45 institutions sont actives dans le domaine de la protection des mineurs contre la cyberdélinquance.

58 mesures ont été identifiées.

22 éseaux / groupes de travail ont été identifiés.

3.3 Analyse documentaire complémentaire sur les mesures en Suisse et dans d'autres pays

En complément aux mesures existantes en Suisse recensées par le biais du questionnaire, une analyse documentaire complémentaire a été menée sur la littérature grise pour détecter d'ultérieures mesures de protection existantes et/ou applicables en Suisse sur les quatre phénomènes (production et distribution de matériel pédopornographique via Internet, cyber grooming, sextorsion, live-streaming d'actes d'ordre sexuel).

Pour cette analyse, des paramètres de recherche ont été prédéfinis afin d'assurer une démarche rigoureuse. Les mesures ont été repérées dans les mois d'octobre à décembre 2021, ainsi qu'en mars 2022 : a) sur la plateforme Jeunes et médias[79] ; b) depuis le moteur de recherche Google, sans limite temporelle ni géographique, en anglais, français, allemand et italien selon quatre combinaisons de mots-clés standardisées dans chacune des langues (Annexe G). Pour être incluses, les mesures doivent : a) être disponibles en anglais, en français, en allemand, ou en italien ; b) traiter d'un des quatre types de cyber-délit discutés dans ce rapport ; c) être accessibles en détails depuis la page de référence ou entre les premiers trois clics. Afin d'analyser les mesures, un certain nombre de variables ont été systématiquement relevées pour chacune de ces mesures, dans la mesure de la disponibilité de l'information[80].

Quelques chiffres sur l'analyse documentaire

188 mesures ont été identifiées, réparties en 29 pays à travers le monde, dont :

24 en Suisse

21 en Grande-Bretagne

20 aux Etats-Unis

17 Belgique

16 anada

[79] Jeunes et médias (https://www.jeunesetmedias.ch/) est la plateforme nationale de promotion des compétences médiatiques mise en place par l'Office fédéral des assurances sociales sur mandat du Conseil fédéral. Son objectif est d'encourager les enfants et les jeunes à utiliser les médias numériques de façon sûre et responsable.

[80] La liste de toutes les mesures recensées peut être consultée dans l'annexe externe disponible en ligne, Sections 3 et 4.

3.4 Entretiens avec des experts de Suisse et d'ailleurs

Afin d'approfondir les données récoltées à travers les recensions de littérature scientifique et grise, ainsi que par le biais des questionnaires, l'équipe de recherche a complété le champ de recherche avec des entretiens menés auprès d'experts non seulement suisses, mais aussi d'autres pays.

Cette activité a été menée sous la forme d'entretiens semi-structurés. Cela signifie qu'une liste de questions potentielles – ou grille d'entretien – a été définie en amont de l'entretien, mais que les chercheurs ont la liberté de poser les questions qui leur semblent pertinentes et d'en ajouter de nouvelles en fonction de la direction que prend la discussion (Annexe E). La grille d'entretien contient 9-10 questions (selon la provenance de l'expert) réparties en quatre blocs thématiques : 1) Questions générales sur l'expert ; 2) Questions générales sur les quatre phénomènes de cyber-délits sexuels et sur les mesures existantes ; 3) Questions spécifiques sur les mesures efficaces, prometteuses ou plutôt inefficaces, et les perspectives ; 4) Partie conclusive.

L'identification des experts s'est basée sur une technique mixte d'échantillonnage non probabiliste (boule de neige) et stratifié. Afin de prendre en compte la diversité des acteurs et experts dans le domaine de la protection des mineurs contre les cyber-délits sexuels, la sélection des experts repose sur les deux critères suivants :

a) *Le champ de compétence* : quatre champs de compétence ont été identifiés et considérés comme étant les plus pertinents, à savoir la prévention sociale, la prévention situationnelle via les solutions techniques, l'investigation policière et la poursuite pénale. Il est à préciser qu'un expert peut recouvrir plus d'un champ de compétence.

b) *Le champ géographique* : tant des experts suisses pour approfondir les connaissances au niveau national que des experts étrangers afin de compléter les renseignements sur les mesures implémentées à l'étranger ont été considérés.

Une invitation à participer à un entretien a été envoyée par courriel[81] à 26 experts au cours des mois de janvier à avril 2022. Après avoir accepté notre invitation, un formulaire d'information et de consentement a été transmis à l'expert (Annexe F). Celui-ci présente les tenants et aboutissants de l'étude, explique ce qui est attendu du participant, et expose les règles en matière de traitement et confidentialité des données. L'expert a pris connaissance du formulaire et retourné une copie signée.

Les entretiens ont été menés sur la plateforme Microsoft Teams. Avec le consentement des interviewés, les entretiens ont été enregistrés directement sur la même plateforme afin de procéder à une retranscription, facilitant ainsi la procédure d'analyse. Les enregistrements sont stockés sur la plateforme, ainsi que sur un ordinateur crypté et protégé par un mot de passe. Conformément au formulaire d'information, les enregistrements seront détruits au plus tard en août 2022.

Alors que le nombre d'entretiens envisagé était d'environ 10, l'équipe de recherche a décidé d'introduire des entretiens supplémentaires.

[81] Une seule invitation a été transmise par courrier postal afin de respecter la procédure standard pour ce type de demande.

Quelques chiffres sur les entretiens

18 experts ont été interviewés dans le cadre de 15 entretiens[82] (9 femmes et 9 hommes).

858 minutes de discussion ont été enregistrées (14,3 heures).

7 entretiens ont été menés en français, 5 en allemand, 3 en anglais.

11 experts proviennent de Suisse, 6 d'Europe[83], et 1 d'Amérique du Nord.

7 experts sont actifs dans le milieu de la police, 3 de la justice, 7 de la prévention sociale et 1 de la prévention situationnelle.

3.5 Croisement des données concernant le contexte suisse

Le croisement des quatre méthodologies décrites ci-dessous ont permis également de dresser le contexte suisse exposé au chapitre 2. En effet, tant les données issues de la littérature – scientifique ou grise –, les questionnaires et les entretiens, ont permis de relever comment le phénomène des cyber-délits sexuels à l'encontre des mineurs est appréhendé au niveau suisse.

Les données ont ensuite été complétées par des sources de données spécialisées. D'une part, les statistiques policières de la criminalité, publiées par l'OFS, ont apporté un portrait chiffré de l'ampleur des infractions enregistrées par la police. D'autre part, la consultation du Code pénal suisse, du Commentaire romand du Code pénal suisse, de la jurisprudence du Tribunal fédéral, ainsi que divers documents publiés par l'administration fédérale a permis de délimiter le cadre législatif en la matière.

[82] Lors de certains entretiens, deux experts étaient présents.
[83] Allemagne, France, Royaume-Uni, Pays-Bas.

4. Résultats

Cette section est organisée en quatre parties. La première partie présente les résultats concernant la revue de littérature des quatre comportements cyberdélinquants : production ou distribution de matériel pédopornographique via Internet (ch. 4.1.1) ; cyber grooming (ch. 4.1.2) ; sextorsion (ch. 4.1.3) ; live-streaming d'actes d'ordre sexuel (ch. 4.1.4). La deuxième partie expose les catégories d'acteurs actifs en Suisse et leurs collaborations selon les informations tirées du questionnaire. La troisième partie reporte les mesures recensées par le biais du questionnaire, de l'analyse documentaire complémentaire et des entretiens. Pour terminer, une quatrième partie présente les résultats des entretiens auprès des experts sur les mesures de protection existantes.

4.1 Les phénomènes dans les études récentes (2016-2021)

Dans ce travail, la littérature récente sur quatre phénomènes a été recensée. Le premier phénomène concerne la production et distribution de matériel pédopornographique via Internet. À travers le deuxième phénomène, il est question du cyber grooming. Le troisième phénomène porte sur la pratique de la sextorsion de mineurs et le quatrième phénomène de ce travail est le live-streaming de pédopornographie. Pour chaque phénomène, les résultats observés dans la littérature ont été classés dans trois dimensions à savoir les dimensions auteurs, victimes et modus operandi.

Dans ce rapport, une synthèse des résultats est présentée pour chaque phénomène à l'étude. Des tableaux synoptiques permettant de résumer les résultats des études pour chacun des phénomènes sont présentés en début de chaque section[84].

[84] Le tableau complet décrivant toutes les études peut être consulté dans l'annexe externe disponible en ligne, Section 1.

4.1.1 Production et distribution de matériel pédopornographique via Internet : auteurs, victimes et modus operandi

Tab. 8 – Résumé des résultats principaux selon les trois dimensions : production et distribution de matériel pédopornographique via Internet (Résumé construit sur la base de 57 manuscrits, dont 17 revues de littérature)

Auteurs	Victimes	Modus operandi
Typologie récurrente : consommateur de pédopornographie ou, en minorité auteur mixte (producteur et consommateur)	Âge des victimes diminue et une aggravation du type de contenu est observable au cours des dernières années selon l'échelle de COPINE[85]	Utilisation de technologies différentes pour échanger du contenu pédopornographique (ex. canaux IRC, des forums du Dark et Clear web ou encore sur des newsgroup)
En majorité des hommes, caucasiens[86], âgés d'environ 40 ans, employés, difficultés dans les relations sociales, personnes avec penchants pédophiles et peu d'antécédents judiciaires	Majoritairement de sexe féminin, âgées de 12-13 ans en moyenne, caucasiennes Plus récemment, changement de cible pour Asie du Sud-est	Distribution de collection de pédopornographie pour obtenir du nouveau contenu et des techniques de recherche
Importance des relations sociales au sein des milieux d'amateurs de pédopornographie sur Internet Rôle de coordinateur joué par les producteurs de pédopornographie	Facteurs de risque : orientation sexuelle LGBTQ+, utilisation de chats rooms et adoption de comportement à risque en ligne/hors-ligne	Choix de la victime selon des critères de vulnérabilité et d'accessibilité, liens familiaux ou sociaux importants entre victimes et producteurs de pédopornographie

Note. 57 manuscrits ont été identifiés pour ce phénomène, dont 17 revues de littérature. Les études empiriques originales sont issues des zones géographiques suivantes : États-Unis (n=9), Australie (n=7), Canada (n=7), Royaume-Uni (n=5), Espagne (n=3), France (n=2), Allemagne (n=1), Finlande (n=1), Nouvelle-Zélande (n=1), Portugal (n=1) et Suisse (n=1). La zone géographique n'a pas pu être déterminée pour deux recherches.

Dans la littérature, la production et distribution de matériel pédopornographique via Internet est définie comme le fait de mettre en acte (1) des actions créatrices de matériel pédopornographique en capturant une/des image(s) ou une/des vidéo(s) à caractère sexuel impliquant des enfants et (2) des actions consistant à partager passivement ou activement ce type de matériel avec d'autres individus, le plus souvent par des TIC[87].

Les populations sur lesquelles les études ont été menées sont : (a) les consommateurs de pédopornographie, (b) les auteurs d'actes d'ordre sexuel (AOS) sur enfants, et (c) les auteurs mixtes. Par consommateur de pédopornographie, il est fait référence à des individus qui consomment du contenu illégal et qui dans certains cas peuvent avoir distribué ce type de matériel. Les auteurs d'AOS sur enfants sont des individus qui ont commis des agressions sexuelles sur enfants et n'ont pas commis d'infractions par Internet. Ces auteurs ne consomment pas ou ne distribuent pas de contenu pédopornographique. Quant aux auteurs mixtes, ils combinent les deux profils précédents.

Au regard de la littérature recensée (57 manuscrits), les recherches effectuées sur les distributeurs et producteurs de pédopornographie se basent sur de données policières ou sur des populations judiciarisées. Pour collecter les données de ces dernières, les outils de sondage, d'entretiens et l'étude de dossiers administratifs sont utilisés. Les données policières fournissent aux chercheurs des bases de données d'images de pédopornographie et de cas de consommation de pédopornographie. Cependant, la littérature recensée s'est peu focalisée sur les populations de producteurs et distributeurs

[85] COPINE est une échelle de sévérité des images de pédopornographie (Annexe C).
[86] Ce terme a été choisi, car il est utilisé dans de nombreuses recherches anglo-saxonnes ou québécoises pour décrire le phénotype des individus en lien avec des infractions de pédopornographie. Dans le contexte européen, ce terme est peu employé. À sa place, certains chercheurs font référence à des individus dont la nationalité est issue du pays où la recherche a été menée.
[87] Fortin, Paquette, et Dupont (2017); Krone (2004).

de pédopornographie. En effet, il est plutôt question de consommateurs de pédopornographie et d'auteurs mixtes[88] pour désigner les populations en lien avec la pédopornographie.

4.1.1.1 Informations sociodémographiques des producteurs et distributeurs de pédopornographie

Basées sur deux revues de littérature, des sondages menés auprès d'auteurs, d'un sondage mené auprès de policiers, d'analyses de dossiers de police, de dossiers judiciaires, de dossiers médicaux, ainsi que sur des entretiens avec des individus reconnus pour des faits de pédopornographie et cela majoritairement dans des contextes anglo-saxons (13/17) avec toutefois quatre recherches issues d'un contexte européen, les recherches recensées se rejoignent sur les caractéristiques sociodémographiques des consommateurs de pédopornographie. Ces derniers sont dans une grande majorité des hommes, âgés d'environ 35-40 ans[89], ils sont majoritairement d'origine caucasienne, ils sont plutôt bien formés (formation de niveau tertiaire) comparés à d'autres groupes d'auteurs tels que les auteurs d'AOS sur enfants[90] et ils ont un emploi[91] au moment de la commission de l'infraction. Certaines des études citées précédemment signalent aussi que d'un point de vue cognitif et affectif, les consommateurs de pédopornographie ont des difficultés à avoir des relations intimes[92], une mauvaise estime de soi[93] et d'affirmation de soi[94].

4.1.1.2 Problématiques psychologiques et sexuelles des producteurs et distributeurs de pédopornographie

Cinq revues de littérature et cinq recherches menées sur de dossiers judiciaires d'auteurs condamnés dont une recherche espagnole ont trouvé que les consommateurs de pédopornographie ont tendance à avoir des attirances sexuelles envers les mineurs et cela dans une proportion plus importante que les auteurs d'AOS sur enfants[95]. De plus, les consommateurs de pédopornographie ont des problèmes de régulation sexuelle[96].

4.1.1.3 Taux de récidive des producteurs et distributeurs de pédopornographie

Le taux de récidive, c'est-à-dire le taux de nouvelle condamnation pour un individu reconnu coupable d'une infraction par le passé, est bas pour les consommateurs de pédopornographie[97]. Ils ont peu

[88] Par consommateurs de pédopornographie, la littérature recensée les différencie des auteurs mixtes qui consomment de la pédopornographie en plus de commettre des actes d'ordre sexuel sur enfants.
[89] Armstrong et Mellor (2016); Brown et Bricknell (2018); Christensen et Tsagaris (2020); Clevenger, Navarro, et Jasinski (2016); Elbert, Drury, et DeLisi (2021); Henshaw, Arnold, Darjee, Ogloff, et Clough (2020); Lacasse (2017); Merdian et al. (2018); Owens, Eakin, Hoffer, Muirhead, et Shelton (2016); (Paquette, 2019); Paquette et Cortoni (2021); Schuhmann (2020); Shelton, Eakin, Hoffer, Muirhead, et Owens (2016); Soldino, Carbonell-Vayá, et Seigfried-Spellar (2019); Steel, Newman, O'Rourke, et Quayle (2021); Ventéjoux (2019).
[90] Brown et Bricknell (2018); Christensen et Tsagaris (2020); DeMarco, Sharrock, Crowther, et Barnard (2018); Henshaw et al. (2020).
[91] Brown et Bricknell (2018); Christensen et Tsagaris (2020); Clevenger, Navarro, et Gilliam (2018); Krone et al. (2017); Lacasse (2017); Owen, Noble, et Speed (2017); Soldino, Carbonell-Vayá, et Seigfried-Spellar (2021).
[92] Armstrong et Mellor (2016); Brown et Bricknell (2018); Clevenger et al. (2018); Lacasse (2017); Owens et al. (2016); Ventéjoux (2019).
[93] Armstrong et Mellor (2016); Bartels et Merdian (2016); Brown et Bricknell (2018); DeMarco et al. (2018); Gottfried, Shier, et Mulay (2020); Paquette (2019); Pugnière-Saavedra (2018); Sheehan (2016); Soldino, Merdian, Bartels, et Bradshaw (2020).
[94] Armstrong et Mellor (2016); Bartels et Merdian (2016); Brown et Bricknell (2018); DeMarco et al. (2018); Gottfried et al. (2020); Paquette (2019); Pugnière-Saavedra (2018); Sheehan (2016); Soldino et al. (2020).
[95] Bartels et Merdian (2016); Brown et Bricknell (2018); Cale, Holt, Leclerc, Singh, et Drew (2021); DeMarco et al. (2018); Elbert et al. (2021); Gottfried et al. (2020); Henshaw (2017); Lamothe (2020); Paquette (2019); Paquette et Cortoni (2021); Soldino et al. (2019); Soldino et al. (2020).
[96] Bartels et Merdian (2016); Brown et Bricknell (2018); Cale et al. (2021); DeMarco et al. (2018); Elbert et al. (2021); Gottfried et al. (2020); Henshaw (2017); Lamothe (2020); Paquette (2019); Paquette et Cortoni (2021); Soldino et al. (2019); Soldino et al. (2020).
[97] Boxall, Pooley, Franks, Long, et Dowling (2021); Brown et Bricknell (2018); Goller, Jones, Dittmann, Taylor, et Graf (2016); Laajasalo, Ellonen, Korkman, Pakkanen, et Aaltonen (2020); Soldino et al. (2021).

d'antécédents judiciaires comparés à d'autres groupes d'auteurs comme les auteurs d'AOS sur enfants ou les auteurs mixtes[98,99]. Une étude menée sur des données judiciaires suisses de la période de 1973 à novembre 2008 a trouvé que la récidive pour des faits de pédopornographie se situe à 1,6%. En comparaison à d'autres formes de délits, cela constitue un faible taux de récidive. En cas de récidive, les consommateurs de pédopornographie ont tendance à consommer du contenu illégal plutôt que de commettre des AOS sur enfants[100]. La recherche suisse mentionnée précédemment a d'ailleurs trouvé que seul 0,2% des consommateurs de pédopornographie devenaient des auteurs mixtes. Deux revues de littérature ainsi qu'une recherche allemande conduite sur des données policières précisent que les auteurs mixtes constituent une minorité des consommateurs de pédopornographie[101].

4.1.1.4 Typologie d'auteurs en lien avec la pédopornographie

Certains consommateurs de pédopornographie peuvent dans certaines situations être des distributeurs de contenu pédopornographie. Ils deviennent des distributeurs passifs lorsqu'ils prennent part à des réseaux pair-à-pair[102]. Sur ce type de réseau, un utilisateur peut partager automatiquement du contenu qu'il aurait téléchargé et cela sans avoir consciemment envoyé ce contenu à un destinataire. Une minorité de consommateurs de pédopornographie devient distributeurs actifs[103], c'est-à-dire qu'il partage consciemment du contenu pédopornographique avec autrui. Dans la sous-culture des amateurs de pédopornographie, la bibliothèque des consommateurs peut servir de monnaie d'échange pour obtenir du nouveau contenu[104]. Leur collection de (pédo)pornographie leur permet aussi d'être reconnus auprès de leurs pairs consommateurs de pédopornographie et d'avoir du prestige dans ce milieu[105].

En plus de s'échanger du contenu, les consommateurs de pédopornographie vont échanger avec d'autres individus sur les meilleures techniques de recherche, car la découverte de contenu par soi-même a des limites[106]. Ces échanges de contenu et de techniques de recherche se déroulent sur une grande variété de plateformes [107] (ex. canaux IRC, des forums du *Dark* et *Clear web* ou encore sur des *newsgroup*). Dans l'ensemble, les consommateurs de pédopornographie sont assez bien éduqués au niveau des TIC[108] et font usage de nouvelles technologies (ex. *Dark* web)[109], mais aussi de technologies plus anciennes (ex. *newsgroup*)[110]. L'utilisation de nouvelles technologies, en particulier celles intégrant des fonctionnalités d'encryptions (ex. Telegram), rendent difficile le travail de la police pour l'identification et l'arrestation des auteurs[111]. Les producteurs de pédopornographie peuvent être qualifiés d'auteurs mixtes, car ils commettent des AOS sur enfants pour produire du contenu pédopornographique. Toutefois, tous les auteurs mixtes ne sont pas forcément des producteurs

[98] DeMarco et al. (2018); Laajasalo et al. (2020); Lacasse (2017); Lamothe (2020); Ly, Dwyer, et Fedoroff (2018); Owens et al. (2016); Soldino et al. (2019).
[99] Gottfried et al. (2020); Massicotte (2016); Napier, Brown, et Smith (2020); Owens et al. (2016); Shelton et al. (2016).
[100] Boxall et al. (2021); Gottfried et al. (2020); Ly et al. (2018).
[101] Fortin et al. (2017); Fortin, Paquette, et Dupont (2018); Schuhmann (2020).
[102] Bissias et al. (2016); Cale et al. (2021); Fortin et al. (2017).
[103] Cale et al. (2021); Clevenger et al. (2018); Fortin et al. (2017); Fortin et al. (2018); Steely, Ten Bensel, Bratton, et Lytle (2018).
[104] Cale et al. (2021); Clevenger et al. (2018); Fortin et al. (2017); Fortin et al. (2018); Steely et al. (2018).
[105] Cale et al. (2021); Fortin et al. (2017); Fortin et al. (2018); Krone et al. (2017).
[106] Fortin et al. (2017); Shelton et al. (2016).
[107] Fortin et al. (2017).
[108] Cale et al. (2021); DeMarco et al. (2018).
[109] Cale et al. (2021); Leclerc, Drew, Holt, Cale, et Singh (2021); Sheehan (2016).
[110] Steel, Newman, O'Rourke, et Quayle (2020).
[111] Cale et al. (2021); Steel et al. (2020).

de pédopornographie. Les auteurs mixtes sont moins bien insérés socialement (ex. plus de chômage ou antécédents criminels plus nombreux) que les consommateurs de pédopornographie (sans contact)[112]. Les auteurs mixtes ont aussi tendance à avoir subi des agressions sexuelles[113]. Une revue de littérature, un sondage de victimisation, deux recherches menées à l'aide d'entretien auprès de producteurs de pédopornographie et une auprès d'intervenants sociaux concluent que dans une grande majorité des cas (97% : chiffre obtenu dans une recherche étatsunienne menée sur des données policières), le producteur de pédopornographie connait personnellement sa victime (ex. famille)[114]. Peu de rencontres entre la victime et le producteur sont organisées par Internet[115].

Un sondage de victimisation ainsi qu'une recherche britannique dont les données sont issues d'entretiens avec des producteurs de pédopornographie (n=22) signalent que les auteurs mixtes choisissent leur victime sur des critères d'accessibilité et de vulnérabilités à la place d'autres critères tels que l'attirance physique[116]. Depuis l'avènement d'Internet ou encore des téléphones portables avec appareil photo, les adultes producteurs peuvent produire du contenu dans des lieux plus variés (ex. dans la chambre de la victime avec une webcam ou dans un parc)[117]. Historiquement, le contenu pédopornographique est produit chez l'auteur[118].

Il reste important de souligner que la production de pédopornographie ne concerne pas que des adultes et des hommes. Les jeunes sont aussi des producteurs et distributeurs de pédopornographie, en particulier lorsqu'ils s'adonnent à la pratique du sexting[119]. Ces jeunes producteurs et distributeurs ne sont toutefois pas le même type d'auteur pédophile décrit ci-dessus. Une seule étude étatsunienne a été menée sur les femmes impliquées dans la production de pédopornographie[120]. Elles agissent en co-auteur avec l'auteur principal qui est un homme. Les victimes sont généralement un/des enfant(s) de la femme.

4.1.1.5 Victimes de pédopornographie

Concernant les victimes, une recherche canadienne menée sur un corpus d'image (n=61'244) de pédopornographie a trouvé que la distribution de leur âge suit une loi normale avec un pic pour les victimes âgées de 10 ans. En comparant des images produites avant l'existence d'Internet et des images produites entre 2008 et 2015, une étude démontre que l'âge moyen des victimes a diminué et la gravité du matériel a augmenté[121]. Plusieurs recherches expliquent que les filles ont plus tendance à être victimisées que les garçons[122]. Une revue de littérature a identifié quatre facteurs qui augmentent le risque de devenir victime en ligne : les antécédents d'abus, l'orientation sexuelle LGBTQ+, l'utilisation de chats rooms et l'adoption de comportement à risque en ligne/hors-ligne[123]. Une majorité des victimes ressemblent aux auteurs en ce qui concerne leur origine ethnique, bien que les

[112] Henshaw, Ogloff, et Clough (2017).
[113] Schuhmann (2020).
[114] Cale et al. (2021); Gewirtz-Meydan, Walsh, Wolak, et Finkelhor (2018); Newton (2021); Sheehan (2016); Shelton et al. (2016).
[115] Shelton et al. (2016).
[116] Gewirtz-Meydan et al. (2018); Sheehan (2016).
[117] Sheehan (2016).
[118] Sheehan (2016).
[119] Molina Martinez (2019).
[120] Bickart, McLearen, Grady, et Stoler (2019).
[121] Salter et Whitten (2021).
[122] DeMarco et al. (2018); Fortin et Proulx (2019); Gewirtz-Meydan et al. (2018); Newton (2021); Quayle, Jonsson, Cooper, Traynor, et Svedin (2018); Salter et Whitten (2021).
[123] DeMarco et al. (2018).

dernières tendances indiquent un changement de cible pour des victimes d'origine d'Asie du Sud-est[124].

4.1.2 Cyber grooming : auteurs, victimes et modus operandi

Tab. 9 – Résumé des résultats principaux selon les trois dimensions : cyber grooming (Résumé construit sur la base de 39 manuscrits, dont 5 revues de littérature)

Auteurs	Victimes	Modus operandi
Typologie récurrente : *contact-driven* et *fantasy-driven*	Majoritairement de sexe féminin, caucasiennes	Stratégies principales : engagement relationnel, tromperie (mentir sur son âge) et corruption (paiements ou dons de cadeaux)
En général, hommes, âgés en moyenne de 35 ans, peu d'antécédents judiciaires	Facteurs de risque : problèmes familiaux et sociaux, problèmes de santé mentale, adoption de comportements à risque, temps passé sur Internet sans supervision, pratiquer le sexting, avoir des inconnus dans ses contacts, jouer aux jeux vidéo et utiliser une messagerie instantanée	En général, forte capacité d'adaptation des auteurs de cyber grooming à leur interlocuteur
Historique de victimisation d'abus sexuels et consommation de pédopornographie	Selon les études, 15% des adolescents ont été sollicités sexuellement sur Internet et 8% ont entretenu des interactions à caractère sexuel par Internet Faible sensibilisation des enfants et adolescents du phénomène de cyber grooming	En général, prise de contact avec les victimes sur les plateformes utilisées par ces dernières (ex. réseaux sociaux) Continuation de la conversation sur service de messagerie instantanée (ex. Snapchat, Skype)

Note. 39 manuscrits ont été identifiés pour ce phénomène, dont cinq revues de littérature. Les études empiriques originales sont issues des zones géographiques suivantes : États-Unis (n=14), Espagne (n=5), Royaume-Uni (n=4), France (n=2), Allemagne (n=2), Australie (n=1), Autriche (n=1), Canada (n=1), Irlande (n=1) et Italie (n=1). La zone géographique n'a pas pu être déterminée pour 11 recherches.

Dans la littérature, le cyber grooming est défini comme la pratique d'individus cherchant à entretenir des relations sexuelles avec des mineures par Internet ou hors ligne (Briggs et al., 2011).

Au total, 39 manuscrits recensés abordent le phénomène du cyber grooming. Selon la littérature recensée, les recherches effectuées sur le cyber grooming sont menées majoritairement à l'aide de retranscriptions de communication entre les auteurs de cyber grooming et des victimes ou des agents infiltrés. Les données proviennent aussi de populations judiciarisées via des sondages ou des entretiens. Lorsque les recherches sont menées sur les victimes de cyber grooming, l'outil du sondage auprès d'un grand échantillon est aussi utilisé.

4.1.2.1 Informations sociodémographiques des auteurs de cyber grooming

Les résultats de cette revue de littérature indiquent que les auteurs de cyber grooming sont âgés d'environ 35 ans[125] et qu'ils sont en grande majorité des hommes[126]. Une recherche menée auprès

[124] Ali, Haykal, et Youssef (2021); Newton (2021).
[125] de Santisteban, del Hoyo, Alcázar-Córcoles, et Gámez-Guadix (2018); DeHart et al. (2017); Drouin, Boyd, et Greidanus Romaneli (2018); Ioannou, Synnott, Reynolds, et Pearson (2018); Joleby, Lunde, Landström, et Jonsson (2021); Kloess, Hamilton-Giachritsis, et Beech (2017); Lorenzo-Dus et Izura (2017); Lorenzo-Dus, Izura, et Pérez-Tattam (2016); Massicotte (2016); Taylor (2017); van Gijn-Grosvenor et Lamb (2016); Winters, Kaylor, et Jeglic (2017).
[126] Chiu, Seigfried-Spellar, et Ringenberg (2018); Clevenger et al. (2018); Davis (2016); de Santisteban et al. (2018); DeHart et al. (2017); Drouin, Boyd, Hancock, et James (2017); Forni et al. (2020); Ioannou et al. (2018); Joleby et al. (2021); Kleijn et Bogaerts (2020); Kloess

d'auteurs connus (n=296) des services de police canadiens a trouvé que les auteurs de cyber grooming n'ont pas ou peu d'antécédents judiciaires[127]. Afin de classifier les auteurs de cyber grooming, deux typologies semblent faire référence dans la littérature.

4.1.2.2 Typologie d'auteurs

La première typologie de Briggs et al. (2011) indique qu'il y a deux groupes d'auteurs : *contact-driven group* (utilisation de l'Internet pour contacter leur victime et les mener à des interactions sexuelles hors ligne) et *fantasy-driven group* (utilisation d'Internet pour commettre des actes sexuels tels que le cybersex, mais sans la volonté de rencontrer les victimes hors ligne).

La seconde typologie de DeHart et al. (2017) est construite en quatre groupes d'auteurs : *cybersex-only offenders* (interactions sexuelles en ligne avec enfants sans planification et exposent facilement leur identité), *schedulers* (planification de rencontre hors ligne pour des interactions sexuelles sans exposer son identité), *cybersex/schedulers* (planification de rencontre en ligne, mais ne se présentent pas au rendez-vous), *buyers* (achat de prestations sexuelles à des enfants ou leurs facilitateurs sans exposer son identité).

Deux revues de littératures expliquent que les auteurs de cyber grooming ont tendance à avoir été victimes d'abus sexuel[128]. Ces auteurs peuvent être qualifiés d'auteurs mixtes, car en plus de vouloir commettre des AOS sur enfants hors ligne ou par Internet, ils consomment de la pédopornographie[129].

4.1.2.3 Modus operandi cyber grooming

Concernant le mode opératoire employé, une enquête espagnole sur un échantillon probabiliste d'élèves d'école secondaire (n=2731) a trouvé que les auteurs de cyber grooming utilisent trois stratégies pour obtenir des relations sexuelles avec la victime[130]. Ces stratégies d'obtention de relations sexuelles sont l'engagement relationnel, la tromperie (mentir sur son âge) et la corruption (paiements ou dons de cadeaux). La stratégie privilégiée pour les victimes de sexe féminin est l'engagement relationnel. Une revue de littérature a identifié quatre modèles de cyber grooming :

- Modèle de O'Connell (2003) : (1) formation d'une relation amicale, (2) formation d'une relation intime, (3) évaluation de risque, (4) étape d'exclusivité, et (5) étape sexuelle.
- Modèle Williams et al. (2013) : (1) développement de liens, (2) contenu sexuel, et (3) évaluation.
- Modèle de Lorenzo-Dus et al. (2016) : (1) accès, (2) piège, et (3) approche.
- Modèle de De Santisteban et al. (2018) : (1) perception de l'Internet comme un environnement facilitant la commission, (2) accéder à la victime, (3) persuasion initiale, (4) victimes et environnement, (5) stratégie de persuasion, et (6) issues sexuelles.

et al. (2017); Lorenzo-Dus et Izura (2017); Lorenzo-Dus et al. (2016); Nikolovska (2020); Quayle (2017); Quayle et Newman (2016); Taylor (2017); van Gijn-Grosvenor et Lamb (2016); Winters et al. (2017).

[127] Massicotte (2016).

[128] Clevenger et al. (2018); Forni et al. (2020).

[129] Fortin et al. (2018); Quayle (2017); Sheehan (2016).

[130] Gámez-Guadix, Almendros, Calvete, et De Santisteban (2018).

Pour reprendre la typologie de Briggs et al. (2011), une recherche australienne basée sur des données policières et un sondage conduit auprès d'auteurs d'infractions sexuelles à l'encontre d'enfants (n=187), ainsi qu'une recherche étatsunienne menée sur des messages entre des auteurs et victimes (n=4353) ont démontré qu'il est possible de distinguer plusieurs phases dans les conversations entre les auteurs *contact-driven* et leurs victimes[131] : formation d'un lien d'amitié/d'intimité, évaluation du risque de se faire découvrir, construction d'une relation exclusive et finalement la relation sexuelle. Ces phases se retrouvent moins chez les auteurs *fanstasy-driven* car, au contraire des auteurs *contact-driven*, ils ne recherchent pas forcément à gagner la confiance de leur victime[132] et ils ne recherchent pas à rencontrer leur victime hors ligne[133].

Concernant les interactions, pendant leurs discussions, certains auteurs de cyber grooming sont capables de s'adapter à leur interlocuteur, selon une revue de littérature et deux recherches qualitatives espagnole et britannique ayant mené des entretiens avec des auteurs (n1=12 ; n2=22)[134]. Par exemple, les auteurs discutant avec des garçons sont plus directs et pressants qu'avec les filles. Deux recherches étatsuniennes menées sur des retranscriptions de conversations ont trouvé que les auteurs font davantage d'efforts pour gagner la confiance des filles[135].

Selon deux recherches étatsuniennes conduites à l'aide de retranscriptions de conversations[136], ce sont plutôt les auteurs de cyber grooming qui ont tendance à mener la conversation et de choisir les sujets abordés que les victimes. Les résultats de trois recherches (Pays-Bas, États-Unis et Canada) conduites sur des retranscriptions de conversations ainsi qu'une revue de littérature signalent que les sujets sexuels sont généralement rapidement introduits dans la conversation[137]. Sur certaines plateformes, la recherche menée aux Pays-Bas ainsi qu'une autre recherche étatsunienne menée à l'aide de retranscriptions de conversations précisent que certains auteurs ont des noms d'utilisateur à connotation sexuelle laissant peu de doute quant à leur intention[138]. Les auteurs hypersexualisés sont plus jeunes que les autres auteurs d'après les résultats d'une étude suédoise dont les données sont issues de l'analyse de 50 rapports d'autorité judiciaire[139]. Aborder des sujets de conversation sexuels, utiliser des termes sexuels et utiliser de la pornographie légale/illégale (y compris la pédopornographie) est à interpréter comme une volonté de l'auteur de désensibiliser la victime à ce type de contenu et de pratiques[140].

D'après deux études étatsuniennes et une étude finlandaise menées sur des retranscriptions de conversations avec des auteurs connus, dont une étude complémentant ses résultats avec des entretiens de policiers, les auteurs de cyber grooming ne mentent pas forcément lors de leur interaction avec les victimes[141]. D'ailleurs, une recherche étatsunienne mentionnée précédemment montre que seule une minorité d'auteurs (1/3) ment sur son âge lors de conversation avec les victimes[142]. Toujours d'après

[131] Chiu et al. (2018); Davis (2016).
[132] Chiu et al. (2018); Davis (2016).
[133] Briggs, Simon, et Simonsen (2011).
[134] de Santisteban et al. (2018); Forni et al. (2020); Sheehan (2016).
[135] Drouin et al. (2017); van Gijn-Grosvenor et Lamb (2016).
[136] Drouin et al. (2018); Drouin et al. (2017).
[137] Bale (2017); Forni et al. (2020); Kleijn et Bogaerts (2020); van Gijn-Grosvenor et Lamb (2016).
[138] Kleijn et Bogaerts (2020); Winters et al. (2017).
[139] Joleby et al. (2021).
[140] Fortin et al. (2018); Lorenzo-Dus et al. (2016); Taylor (2017).
[141] Broome, Izura, et Davies (2020); Nikolovska (2020); Winters et al. (2017).
[142] Winters et al. (2017).

cette étude étatsunienne, lorsque les auteurs de cyber grooming mentent sur leur âge, ils se présentent comme étant plus jeunes de ce qu'ils sont, mais aucun ne se présente comme étant un enfant[143].

Suivant les résultats d'une revue de littérature, de deux sondages conduits en Allemagne et Autriche auprès de jeunes adultes et jeunes d'école secondaire, d'une étude britannique ayant analysé les conversations entre auteurs et victimes et d'une étude tchèque ayant travaillé notamment sur des cas de cyber grooming détectés par la police, les auteurs se connectent sur des plateformes en ligne utilisées par leurs cibles afin d'entrer en contact avec elles[144]. Aujourd'hui, ces plateformes sont principalement des réseaux sociaux, mais il est possible de retrouver des auteurs sur des jeux vidéo en ligne[145], des chats rooms[146] ou encore des services de live-streaming[147] (ex. Omegle). Après le contact initial sur ces plateformes, les auteurs redirigent parfois les victimes vers des services de messagerie instantanée (ex. Snapchat, Skype)[148].

4.1.2.4 Victimes de cyber grooming

En ce qui concerne les victimes, les filles sont plus à risque d'être la cible de cyber grooming que les garçons[149]. Trois sondages de victimisation conduits en Europe sur une population de jeunes d'école secondaire et une revue de littérature indiquent que des facteurs de vulnérabilité sont des problèmes familiaux, sociaux, de santé mentale et des victimisations précédentes d'abus sexuels[150]. Selon un sondage de victimisation (n=1196) mené au Royaume-Uni, en Italie et en Irlande, les jeunes adoptant des comportements à risque en ligne et hors ligne (ex. consommation de stupéfiant) ont plus tendance à être victimes de cyber grooming[151]. Une revue de littérature a mis l'accent sur le fait que les activités routinières suivantes augmentent le risque de devenir victime de cyber grooming : le temps passé de manière non supervisée dans certains endroits du cyberespace (ex. plateformes de jeu vidéo, messagerie instantanée), la pratique du sexting, et accepter des inconnus parmi ses contacts. [152]

Deux études qualitatives conduites en analysant des retranscriptions de conversation et une étude basée sur des entretiens avec des victimes montrent que les victimes s'engagent avec les auteurs pour des questions de curiosité et d'expérimentation sexuelle[153].

[143] Winters et al. (2017).
[144] DeMarco et al. (2017); Kloess et al. (2017); Kopecký (2017); Nikolovska (2020); Weingraber, Plath, Naegele, et Stein (2020); Zöchbauer (2021).
[145] Forni et al. (2020).
[146] DeMarco et al. (2018).
[147] Rodríguez, Durán, Díaz-López, Pastor-Galindo, et Mármol (2020).
[148] Kloess et al. (2017); Nikolovska (2020); Rodríguez et al. (2020); Winters et al. (2017).
[149] Clevenger et al. (2018); de Santisteban et al. (2018); DeMarco et al. (2017); Forni et al. (2020); Ioannou et al. (2018); Joleby et al. (2021); Kloess et al. (2017); Quayle et Newman (2016); Weingraber et al. (2020).
[150] de Santisteban et Gámez-Guadix (2018); DeMarco et al. (2017); Forni et al. (2020); Machimbarrena et al. (2018).
[151] de Santisteban et Gámez-Guadix (2018); DeMarco et al. (2017).
[152] Forni et al. (2020).
[153] Joleby, Lunde, Landström, et Jonsson (2020); Kloess et al. (2017); Seymour-Smith et Kloess (2021).

4.1.3 Sextorsion (sur mineurs) : auteurs, victimes et modus operandi

Tab. 10 – Résumé des résultats principaux selon les trois dimensions : sextorsion sur mineurs (Résumé construit sur la base de 10 manuscrits, dont 1 revue de littérature)

Auteurs	Victimes	Modus operandi
En général, hommes, plus âgés que la victime	Sexe féminin majoritaire et orientation sexuelle non exclusivement hétérosexuel plus à risque	Capture d'image lors de relations intimes pour forcer la réconciliation ou humilier la victime Capture d'image lors de relation par Internet pour forcer l'envoi de contenu à caractère sexuel
Selon les études relevées, 1,9 – 3% des adolescents sont auteurs de sextorsion	Environ 5% de la population d'adolescents sont victimes de sextorsion	En général, la mise à exécution des menaces (diffusion des images/vidéos) dans presque la moitié des cas (45%) Auteurs connaissant la victime ont plus tendance à mettre en œuvre leur menace
Les études relèvent que parfois les auteurs de sextorsion ont également été victimes de sextorsion	Taux bas de dénonciation et peu de recours à l'aide extérieur Freins à la dénonciation ou au recours à l'aide : honte et risques judiciaires de poursuite pour des faits de pédopornographie	Intensification des menaces en cas de non-coopération de la victime Risque important de victimisation ultérieur en cas de coopération de la victime

Note. 10 manuscrits ont été identifiés pour ce phénomène, dont une revue de littérature. Les études empiriques originales sont issues des zones géographiques suivantes : États-Unis (n=4) et de la République tchèque (n=1). La zone géographique n'a pas pu être déterminée pour quatre recherches.

Dans la littérature, la sextorsion est définie comme une forme de chantage en utilisant des images ou vidéos à caractère sexuel d'une victime[154].

Au total, 10 manuscrits ont été recensés. Les recherches effectuées sur la sextorsion sont menées majoritairement à l'aide de sondages de victimisation conduits auprès de jeunes d'école secondaire. Une seule revue de littérature a été recensée. En comparaison aux deux phénomènes précédents, la sextorsion sur mineurs est moins explorée par la communauté académique.

4.1.3.1 Informations sociodémographiques des auteurs de sextorsion

Une revue de littérature, une recherche menée aux États-Unis et une recherche menée en République tchèque montrent que les auteurs de sextorsion sont majoritairement des hommes[155]. En se basant sur une analyse de 25 cas issus de données policières, une recherche tchèque situe l'âge des auteurs adultes de sextorsion dans l'intervalle 28 à 39 ans[156]. Même si l'âge est peu mentionné, une revue de littérature relève que les auteurs de sextorsion sont plus âgés que leur victime et cela notamment pour le cas d'auteurs mineurs[157].

Une étude étatsunienne menée à l'aide d'un échantillon probabiliste (n=5'568) indique que 5% d'élèves d'école secondaire sont victimes de sextorsion, alors que 3% de l'échantillon a commis des actes pouvant être qualifiés de sextorsion. Une autre étude tchèque menée sur une population similaire, elle aussi sur la base d'un échantillon probabiliste (n=21'372), a trouvé que 6,46% de l'échantillon est

[154] O'Malley et Holt (2020); Wolak et Finklelhor (2016).
[155] Charles (2017); Kopecký (2017); Patchin et Hinduja (2020).
[156] Kopecký (2017).
[157] Charles (2017).

victime de chantage et que 1,9% de l'échantillon en est auteur[158]. L'étude étatsunienne citée précédemment signale qu'il y a un fort lien entre commission de sextorsion et victimisation par sextorsion [159]. Les auteurs de sextorsion ont tendance à avoir été victimes de cette pratique. Deux tiers des auteurs ont été victimisés de cette façon d'après la recherche étatsunienne citée ci-dessus.

4.1.3.2 Modus operandi sextorsion

Les raisons poussant les auteurs à commettre cette pratique sur les mineurs sont[160] :

- suite à des images capturées lors d'une relation intime, les auteurs veulent forcer une réconciliation avec la victime ou l'humilier.
- suite à des images capturées lors d'une relation/interaction par Internet, l'auteur utilise des images pour forcer la victime à lui envoyer du contenu similaire ou à avoir des relations sexuelles.

Les études analysées indiquent que les menaces proférées par les auteurs sont mises à exécution dans 45% des cas[161]. Les auteurs connaissant les victimes hors ligne ont plus tendance à publier le contenu[162]. En cas de résistance de la part des victimes, les auteurs intensifient leur menace[163]. Malgré tout, plus la victime coopère avec l'auteur, plus l'auteur peut forcer la victime à subir/commettre des actes qualifiés de graves[164]. Les cas de sextorsion entre un auteur et une victime s'étant rencontrés par Internet se produisent généralement après le cyber grooming[165]. Cependant, plus de 80% des cas de sextorsion concernent une victime connaissant l'auteur hors ligne, selon deux études étatsuniennes[166]. Une étude menée auprès d'experts en cybercriminalité étatsuniens (n=5) indique que les cas de piratage de l'ordinateur de la victime sont rares[167].

4.1.3.3 Victimes de sextorsion

Concernant les victimes, les études recensées se sont concentrées sur des victimes adolescentes (11-17 ans) ou des personnes ayant été victimisées pendant leur adolescence[168]. Les adolescentes sont surreprésentées parmi les victimes[169]. Les adolescents masculins non exclusivement hétérosexuels ont deux fois plus de risque d'être victimes de sextorsion que les adolescents masculins hétérosexuels[170]. Une recherche menée aux États-Unis sur la base d'un échantillon probabiliste (n=5568) de la population d'élèves de niveau scolaire secondaire montre que seul 34% des victimes dénoncent le cas de sextorsion à la police, à un parent ou une personne du système scolaire[171]. Une autre étude étatsunienne menée sur la base d'un échantillon non-probabiliste (n=1631) signale que seul 20% de l'échantillon a recouru à une aide extérieure (ex. police, site Internet ou application gérant les échanges

[158] Kopecký (2017); Patchin et Hinduja (2020).
[159] Patchin et Hinduja (2020).
[160] O'Malley et Holt (2020); Wolak et Finklelhor (2016).
[161] Wolak et Finklelhor (2016).
[162] Wolak et Finklelhor (2016).
[163] Kopecký (2017); Lightfoot (2016); Seymour-Smith et Kloess (2021); Wolak et Finklelhor (2016).
[164] Kopecký (2017); O'Malley et Holt (2020).
[165] Kopecký (2017); O'Malley et Holt (2020); Seymour-Smith et Kloess (2021).
[166] Patchin et Hinduja (2020); Wolak et Finklelhor (2016).
[167] Lightfoot (2016).
[168] Charles (2017); Joleby et al. (2020); Kopecký (2017).
[169] Charles (2017); Joleby et al. (2020); Kopecký (2017); O'Malley et Holt (2020); Patchin et Hinduja (2020); Wolak et Finklelhor (2016).
[170] Patchin et Hinduja (2020).
[171] Patchin et Hinduja (2020).

entre l'auteur et la victime)[172]. Le sentiment de honte et la menace d'être poursuivies pour des faits de pédopornographie retiennent les victimes[173]. Ces dernières sont fortement affectées psychologiquement[174].

4.1.4 Live-streaming de contenu pédopornographique : auteurs, victimes et modus operandi

Tab. 11 – Résumé des résultats principaux selon les trois dimensions : live-streaming de contenu pédopornographique (Résumé construit sur la base de 4 manuscrits)

Auteurs	Victimes	Modus operandi
En prévalence hommes, âgés entre 50 et 69 ans	En prévalence victimes issues des Philippines et des milieux défavorisés	En moyen, les auteurs prolifiques dépensent moins de 55$ par transaction Transactions effectuées à travers des services de rémittence
En général, peu d'antécédents judiciaires en lien avec des infractions sexuelles	La gravité du contenu pornographique est entre le niveau 6 (pose érotique) à 10 (abus sado-maso et AOS sur enfants) selon l'échelle de COPINE	En général, contenu visionné sur des plateformes grand public (ex. Viber, Skype)
Un petit nombre d'auteurs est responsable de la majorité des transactions en lien avec les live-streaming pédopornographiques	-	Il y a des facilitateurs qui organisent la rencontre entre auteurs et victimes

Note. Quatre manuscrits ont été identifiés pour ce phénomène. Les études empiriques originales sont issues des zones géographiques suivantes : Australie (n=3). La zone géographique n'a pas pu être déterminée pour une recherche.

Dans la littérature, par live-streaming, il est entendu le visionnement de contenu pédopornographique en temps réel[175] .

Au total, 4 manuscrits ont été recensés. Les recherches effectuées sur le live-streaming de pédopornographie sont menées majoritairement à l'aide de données policières australiennes. Aucune revue de littérature n'a été recensée. Au vu du petit nombre de publications recensées et du caractère récent de ces publications, il semblerait que la communauté académique ne s'intéresse que depuis peu à ce phénomène. Le savoir académique sur ce dernier est donc faible. Par exemple, il y a très peu d'informations au sujet des victimes et de la pratique du live-streaming dans le monde.

Les consommateurs de *live streams* pédopornographiques sont des hommes, caucasiens, majoritairement âgés de 50 à 69 ans[176]. La majorité des consommateurs de *live streams* ont peu d'antécédents judiciaires en lien avec des infractions sexuelles[177].

Un petit nombre d'auteurs est responsable de la majorité des transactions en lien avec les *live streams* pédopornographiques[178]. Ces auteurs ont plus d'antécédents judiciaires[179]. Selon les études recensées, ces auteurs prolifiques dépensent moins de 55$ par transaction[180]. Les victimes résidant aux Philippines et étant issues de milieux défavorisés, ces transactions se font via des services de

[172] Charles (2017); Patchin et Hinduja (2020); Wolak et Finklelhor (2016).
[173] Wolak et Finklelhor (2016).
[174] Charles (2017); Joleby et al. (2020).
[175] Napier, Teunissen, et Boxall (2021).
[176] Napier et al. (2020); Napier et al. (2021).
[177] Napier et al. (2020).
[178] Cubitt et Napier (2021).
[179] Napier et al. (2020).
[180] Cubitt et Napier (2021); Napier et al. (2021).

rémittence[181]. Certains auteurs interagissent directement avec les victimes, mais la majorité des auteurs ont des contacts avec des facilitateurs (individus facilitant la mise en œuvre d'une session de *live stream*)[182]. Le contenu est visionné sur des plateformes grand public (ex. Viber, Skype,)[183]. Le type de contenu est classifiable du niveau 6 (pose érotique) au niveau 10 (abus sado-maso et AOS sur enfants) de l'échelle de COPINE[184].

4.2 Les acteurs du domaine de la protection des enfants et des jeunes en Suisse

Cette section présente, d'une part, les acteurs qui sont actifs en Suisse dans la protection des enfants et des jeunes en matière de cyberdélinquance sexuelle et, d'autre part, les collaborations et réseaux traitant également de cette thématique. Les résultats reposent sur une analyse croisée de toutes les sources de données utilisées dans le cadre de cette étude (données en accès libre des analyses documentaires, questionnaire, entretiens, autre[185]). Le recoupement de données a permis d'étendre la portée des résultats, mais ne prétend pas pour autant fournir une liste exhaustive des acteurs et des collaborations actifs en Suisse, dès lors que certaines informations ont pu échapper aux méthodes de collectes de données[186].

4.2.1 La pluralité des acteurs actifs

La protection des mineurs relative aux cyber-délits sexuels est une thématique de grande importance pour plusieurs secteurs d'activité. L'engagement des institutions peut se déployer sous plusieurs formes : en organisant une initiative, en participant à une initiative ou en faisant appel à une institution tierce pour mener une initiative (partenariat de prestation).

Au total, nous avons identifié 76 institutions actives dans ce domaine en Suisse. Les institutions sollicitées et détectées dans le cadre de l'étude peuvent être regroupées en cinq catégories (Fig. 1)[187].

(a) Le milieu scolaire (écoles publiques, écoles privés)

(b) Les corps de police

(c) Les départements et offices des gouvernements (à l'échelle communale, cantonale et nationale)

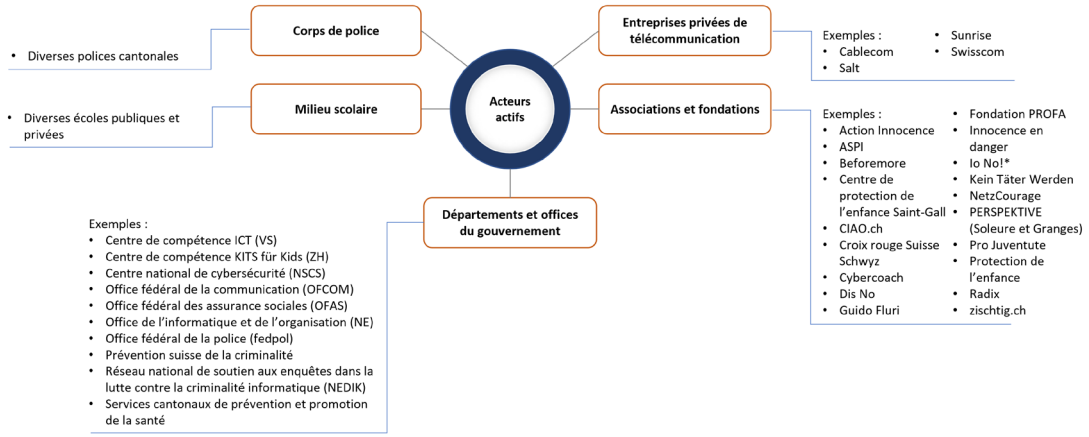
(d) Les associations et fondations

(e) Les entreprises de télécommunication

Nous décrivons chacune de ces catégories dans les paragraphes suivants.

[181] Napier et al. (2020).
[182] Napier et al. (2021).
[183] Napier et al. (2021).
[184] Napier et al. (2021).
[185] Par autre, nous entendons les informations obtenues via un autre canal dans le cadre des activités de recherche, par exemple: discussions avec des collègues, médias, recherche libre.
[186] Plusieurs hypothèses peuvent être formulées : (1) l'information n'est pas publique ; (2) l'information n'est pas publiée sur Internet ; (3) l'information n'a pas été détectée par les mots clés de recherche ; (4) l'information n'a pas été fournie dans le cadre du questionnaire ou des entretiens.
[187] Précisons que les tribunaux ont également été investigués, mais aucune initiative n'a été relevée.

Fig. 1 – Acteurs actifs en Suisse identifiés dans l'étude



* Cette figure se fonde sur les données récoltées entre décembre 2021 et mai 2022. L'association Io No! sera prochainement rattachée à l'association Dis No.

a) Le milieu scolaire

En tant que lieu d'accueil et d'éducation des enfants et des jeunes, les écoles sont actives en vue de les protéger. Les écoles indiquent principalement des leçons de sensibilisation qui sont souvent conduites par des tiers, tels que :

- une association ou une fondation de la société civile, par exemple Action Innocence, Fondazione Aiuto, Sostegno e Protezione dell'Infanzia (ASPI), Croix rouge du canton de Schwyz, Cybercoach, Fondation PROFA, Kinderschutzzentrum Saint-Gall, Protection de l'enfance Suisse, PERSPEKTIVE (région Soleure et Granges), Pro Juventute, Radix, zischtig.ch ;
- une organisation privée de télécommunication, comme par exemple Swisscom ; ou
- un corps de police (*infra*, section b).

Quant au contenu, les cyber-délits sexuels sont généralement abordés dans le cadre d'interventions plus larges portant sur l'éducation numérique ou les dangers d'Internet et des réseaux sociaux. Seuls trois programmes visant spécifiquement une sensibilisation sur l'un des quatre phénomènes ou sur la thématique « violence sexuelle et Internet » ont été relevés. Le cyber grooming et la pornographie sont les plus souvent mentionnés, suivis par la sextorsion. Ces thématiques sont plutôt discutées avec les adolescents qu'avec les enfants plus jeunes. En revanche, aucun cours ou programme évoquant le live-streaming n'a été relevé. Cela ne signifie pas pour autant qu'aucune prévention n'est faite à cet égard. Précisons encore que plusieurs interventions scolaires ont été écartées de l'analyse car portant expressément sur le cyber harcèlement ou le sexting.

En complément, certaines formules incluent également une rencontre avec les parents afin de leur transmettre les mêmes messages.

Une autre activité entreprise par les écoles relève de l'installation de logiciel de contrôle parental et de pare feu sur les ordinateurs à disposition dans l'enceinte de l'école, ainsi que l'élaboration de charte de sécurité quant à l'utilisation du matériel informatique.

Le milieu scolaire semble donc principalement faire appel à des initiatives visant à renforcer l'éducation numérique en général, la prévention de la victimisation[188], l'information aux parents et la protection informatique.

b) Les corps de police

Au-delà des actions répressives et d'enquête, l'activité des corps de police inclut également un pan préventif. Comme relevé plus haut, plusieurs corps de police – division prévention ou brigade des mineurs – se déplacent dans les salles de cours d'école pour sensibiliser les élèves à la bonne utilisation d'Internet et des dangers qu'ils peuvent y rencontrer[189]. Les phénomènes couverts par ces interventions ne sont pas toujours précisés, mais le cyber grooming est le comportement le plus souvent nommé.

De plus, les corps de police réalisent ou diffusent également des campagnes de prévention et mettent à disposition des informations sur leurs sites Internet. Ils sont donc actifs dans la répression de la criminalité, la prévention de la victimisation des jeunes (y compris l'information aux parents) et l'aide aux victimes.

c) Les départements et offices des gouvernements (à l'échelle communale, cantonale et nationale)

Au niveau cantonal, les départements et offices compétents sont en charge de la gestion de l'instruction publique. Dans certains cas, les mandats de prestation avec des organisations tierces ou les collaborations avec les corps de police pour les cours de sensibilisation en milieu scolaire sont initiés par eux.

En outre, que ce soit le département de la formation, de la santé ou de la sécurité, certaines directions ont créé des plateformes en ligne mettant à disposition des jeunes et des parents des informations sur la thématique des nouvelles technologies. Avec une dimension plus interactive, des blogs sont également apparus. Nous pouvons citer par exemple le centre de compétence ICT (Valais), le centre compétence KITS für Kids (ville de Zürich), et l'Office de l'informatique et de l'organisation (Neuchâtel) avec la plateforme PrévenTIC.

D'autre part, ces acteurs étatiques peuvent également assurer la protection du matériel informatique utilisé dans les écoles obligatoires en installant des logiciels de contrôle parental et des pares feu.

Enfin, mentionnons que les services de prévention et promotion de la santé des cantons d'Appenzell Rhodes-Extérieures, des Grisons, de Nidwald, de Saint-Gall, de Schaffhouse, de Schwyz, de Thurgovie, de Zoug et de Zurich[190] se sont associés pour élaborer le programme de prévention Freelance qui comprend un module de prévention sur les médias numériques incluant le cyber grooming et la pornographie. Le programme organise également un concours d'affiche[191].

[188] Par prévention de la victimisation nous entendons, au sens large, l'ensemble des mesures qui ont pour objectif d'éviter que les individus deviennent victimes d'un délit ou d'une infraction.
[189] L'étude a identifié de telles interventions auprès des polices cantonales suivantes : Bâle Campagne, Bâle Ville, Berne, Genève, Neuchâtel, Obwald, Schaffhouse, Schwyz, Soleure, Thurgovie, Valais, Vaud, Zoug. A nouveau, certains corps de police intervenant dans le milieu scolaire n'ont pas été cités ici car les informations à disposition portaient sur une sensibilisation centrée sur le cyber harcèlement, le sexting, ou l'éducation numérique en général.
[190] La principauté du Lichtenstein fait également partie de ce groupement.
[191] Le cyber grooming, la pornographie, le sexting et le cyber harcèlement font partie des thèmes envisageables pour l'affiche.

Au niveau fédéral, l'Office fédéral de la communication (OFCOM), en collaboration avec d'autres offices fédéraux et la PSC, a publié des courtes bandes dessinées sur divers thèmes liés à l'Internet, dont le cyber grooming. Mentionnons également l'Office fédéral des assurances sociales (OFAS) qui, sur mandat du Conseil fédéral, a créé la plateforme Jeunes et médias pour la promotion des compétences numériques. Jeunes et médias travaille dans trois champs d'action : l'information et sensibilisation des parents, professionnels et personnes de références des enfants et des jeunes ; le développement du savoir et des compétences (conseil et expertise, soutien à des projets ou recherches) et la coordination et réseau (organisation de manifestations, participation à des groupes de spécialistes)[192]. Ensuite, mentionnons que la Prévention suisse de la criminalité (PSC), un service intercantonal spécialisé dans les domaines de la prévention de la criminalité et de la promotion de la sûreté, est également active en publiant des brochures, flyers et vidéos sur plusieurs cyber-délits sexuels (cyber grooming, sextorsion, pornographie). Nous relevons également que plusieurs sites Internet, de gouvernance étatique ou autre, renvoient au site de la PSC ainsi qu'à la plateforme Jeunes et médias pour obtenir des informations complémentaires.

Toutes ces institutions sont dès lors actives dans la prévention de la victimisation des jeunes, l'information aux parents, et la protection informatique.

En complément à ces initiatives, la police fédérale (fedpol), ainsi que le Centre national pour la cybersécurité (NCSC) ont mis en place des plateformes de signalement. Alors que la première est consacrée à la notification de matériel de pornographie interdite sur Internet, la seconde permet la dénonciation de tout type de cyber-délit. Néanmoins, les signalements concernant de la pédopornographie qui arrivent au NCSC sont transmis directement à fedpol.

d) Les associations et fondations

Plusieurs associations et fondations se sont engagées dans la protection des enfants et des jeunes face aux risques d'Internet, couvrant également la violence sexuelle.

Comme déjà mentionné, certaines organisations proposent de sensibiliser les jeunes à la thématique – et parfois même les adultes (enseignants, parents, professionnels) – sous forme d'interventions en milieu scolaire, de conférences ou d'ateliers, comme par exemple, Action Innocence, ASPI, Centre de protection de l'enfance de Saint-Gall (créé par l'hôpital pour enfants de Suisse orientale)[193], Croix rouge Suisse du canton de Schwyz, Cybercoach, Fondation PROFA, PERSPEKTIVE (région Soleure et Granges), Pro Juventute, Protection de l'enfance Suisse, Radix, zischtig.ch. Les initiatives de sensibilisation peuvent également prendre la forme d'exposition itinérante, comme par exemple l'exposition « I säg was lauft » construite par le Centre de protection de l'enfance de Saint-Gall, qui a maintenant été reprise par la Fondation de Protection de l'enfance Suisse (Mon corps est à moi !, Love limits). Enfin, des jeux didactiques sont également conçus pour sensibiliser les jeunes à des thématiques, comme le jeu « Datosphäre » – développé par le Centre de protection de l'enfance de Saint-Gall – qui porte principalement sur la protection des données, la sphère privée et l'image de soi publique.

[192] https://www.jeunesetmedias.ch/platforme/la-plateforme-nationale-jeunes-et-medias
[193] Das Kinderschutzzentrum (KSZ) des Ostschweizer Kinderspitals.

En revanche, d'autres institutions mettent à disposition des informations via des brochures ou des plateformes en ligne, comme CIAO.ch, iBarry.ch[194], Pro Juventute (147.ch), et Protection de l'enfance. Les offres précédentes sont complétées par les services d'aide et de soutien (sans option de traitement), où les enfants et les jeunes – voire les parents – peuvent contacter une permanence via téléphone, chat, SMS et e-mail, comme par exemple CIAO.ch, le Centre de protection de l'enfance de Saint-Gall, et Pro Juventute (147.ch). Alors que ces derniers s'orientent davantage vers les victimes (potentielles) ou leurs proches, des institutions proposent des services d'aide et soutien (sans option de traitement) – via téléphone ou e-mail – pour les auteurs (potentiels) et leur entourage, comme par exemple Dis No, Beforemore, Io No ![195] et Kein Täter werden.

En complément à ces services, des associations et fondations, comme par exemple Protection de l'enfance Suisse, Guido Fluri et NetzCourage, ont également investi dans des plateformes de signalement pour dénoncer du matériel pédopornographique.

Enfin, des institutions contribuent à la protection des mineurs en réalisant des recherches afin d'approfondir l'état des connaissances et des pratiques en la matière, telle qu'Innocence en danger.

e) Les entreprises privées de télécommunication

En tant que fournisseurs de services de télécommunication, ces entreprises privées sont également impliquées dans la protection des enfants et des jeunes face aux dangers liés à l'utilisation de ces services. L'art. 46a al. 3 de la Loi sur les télécommunications (LTC)[196], entrée en vigueur le 1er janvier 2021, stipule que les fournisseurs de services de télécommunication ont l'obligation, d'une part, de supprimer « les informations à caractère pornographique au sens de l'art. 197, al. 4 et 5. du code pénal qui leur sont signalées par l'Office fédéral de la police » (1e phrase) et, d'autre part, de signaler à « l'Office fédéral de la police les cas suspects d'informations à caractère pornographique au sens de l'art. 197, al. 4 et 5, du code pénal qu'ils découvrent fortuitement dans le cadre de leurs activités ou que des tiers ont portés à leur connaissance par écrit » (2e phrase).

Ensuite, mentionnons l'initiative sectorielle « Protection de la jeunesse dans les médias » introduite en 2008 et signée par Quickline, Salt Mobile, Sunrise UPC et Swisscom. A travers cette initiative sectorielle, les entreprises signataires s'engagent à appliquer d'office, ou mettre à disposition de leurs clients, des mesures techniques et professionnelles (par ex. sets de blocage, filtres Internet), de prévention et d'information[197].

D'autre part, Swisscom mène aussi des interventions dans le milieu scolaire et finance tous les deux ans l'étude JAMES portant sur l'utilisation des outils technologiques par les jeunes.

[194] La plateforme iBarry a été créée par Swiss Internet Security Alliance. Bien que ce soit une initiative du milieu de l'industrie, les polices cantonales ainsi que le NCSC y sont associés.
[195] Ces informations se fondent sur les données récoltées entre décembre 2021 et mai 2022. L'association Io No! sera prochainement rattachée à l'association Dis No.
[196] RS 784.10. Entrée en vigueur le 30 avril 1997.
[197] asut (2021).

4.2.2 Les réseaux et groupes de travail mis en place

L'exposé des acteurs a permis d'ores et déjà de souligner plusieurs collaborations, notamment dans le milieu scolaire qui est un terrain propice à la prévention auprès des enfants et des jeunes et à l'intervention de partie tierce. D'autres collaborations sont plus ou moins formalisées sous forme de réseaux professionnels ou de groupes de travail. L'étude a permis d'identifier 22 réseaux ou groupes de travail. Lorsque les données étaient accessibles, des informations quant aux membres, à la portée géographique et aux objectifs ont été répertoriées[198].

Les réseaux détectés proviennent principalement des réponses du questionnaire. En effet, il est plus simple d'obtenir ce type d'information directement auprès des institutions concernées car elles sont plutôt difficiles à détecter dans les sources ouvertes. Trois raisons peuvent être avancées : (1) le champ couvert par le réseau est plus large et les cyber-délits sont une thématique parmi d'autres ; (2) le réseau professionnel ne fait pas l'objet de publication sur Internet ; (3) la collaboration ou le réseau est peu formalisé.

De manière générale, les réseaux ou groupes de travail n'ont pas de nom formel. De plus, les réseaux et groupes de travail cités par les répondants portent généralement sur des thématiques plus larges telles que l'éducation numérique dans les écoles, la prévention de la violence, la protection de la jeunesse, etc. Les cyber-délits y sont donc probablement abordés parmi d'autres thématiques. Seuls deux groupes de travail et deux réseaux semblent se rapprocher le plus de la thématique à l'étude.

- Le **réseau national de la Prévention suisse de la criminalité (PSC)**. Il réunit les polices cantonales et communales suisses (responsables prévention), fedpol, divers acteurs étatiques et cantonaux, et des ONG. Il vise à renforcer la coopération policière intercantonale dans le domaine de la prévention de la criminalité, identifier les phénomènes criminels, et proposer des campagnes de prévention pour toute la Suisse. Des groupes de travail spécifiques aux délits, de même que des groupes permanents, sont mis en place. Nous pouvons présumer que les cyber-délits sont fréquemment discutés au sein du réseau.
- Le **réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK)**. Pour plus d'informations, nous renvoyons le lecteur au ch. 2.3.2.
- Le **groupe de travail du Concordat Latin portant sur la cybercriminalité et la lutte contre le pédocriminalité** : regroupant des spécialistes de police des cantons romands et Berne[199], il a pour objectif de mettre en commun les connaissances et de renforcer la formation et la coordination dans le cadre des cyberpatrouilles d'enquêteurs sur Internet pour lutter contre les pédocriminels.
- Le **groupe de travail national « sexualité et médias numériques »** : il est composé de sept membres (Action Innocence, Peer-Campaigns, Pro Juventute, Protection de l'enfance Suisse, SANTE SEXUELLE Suisse, Sexualberatung Bern, Zischtig.ch). Dans une perspective préventive, ce groupe travaille sur la base d'un document de positionnement[200], afin d'encourager les compétences numériques des enfants et des jeunes pour qu'ils puissent

[198] La liste de tous les réseaux identifiés peut être consultée dans l'annexe externe disponible en ligne, Section 2.
[199] Bien qu'il s'agisse d'une initiative du Concordat Latin, le canton du Tessin ne participe pas à ce groupe de travail à l'heure actuelle.
[200] https://www.jeunesetmedias.ch/fileadmin/PDFs/Experten/Doc_positionnement_sexualite_medias_numeriques.pdf

profiter des opportunités données par les médias en ce qui concerne la sexualité et, en même temps, faire face aux défis et risques. Il se réunit trois fois par an en ligne. Ses membres échangent sur la thématique et organisent des manifestations.

En outre, ces réseaux et groupes de travail privilégient l'échange de connaissances et de pratiques interdisciplinaires. Cependant, les descriptifs fournis dans le questionnaire étant relativement pauvres, aucune autre considération ne peut être formulée sur les objectifs et les activités poursuivis par ces réseaux et groupes de travail.

Enfin, quant à la portée géographique, les réseaux et groupes de travail s'inscrivent davantage dans une perspective nationale, cantonale, voire intercantonale. Peu d'initiatives locales ont été indiquées par les répondants.

4.3 Les mesures visant à protéger les enfants et les jeunes en Suisse et ailleurs

Cette section présente les mesures de protection identifiées en Suisse et dans d'autres pays. Elles ont été identifiées à travers un questionnaire adressé à des institutions suisses, une recherche de littérature grise, ainsi que par le biais d'entretiens menés avec des experts suisses et européens. L'inventaire des mesures a finalement été complété avec des mesures découvertes de manière fortuite dans le cadre des activités de recherche[201]. À nouveau, que ce soit pour la Suisse ou à l'extérieur, les résultats apportent une vue d'ensemble sur les diverses offres en matière de protection des enfants et des jeunes, mais ne fournissent pas une liste exhaustive des mesures existantes.

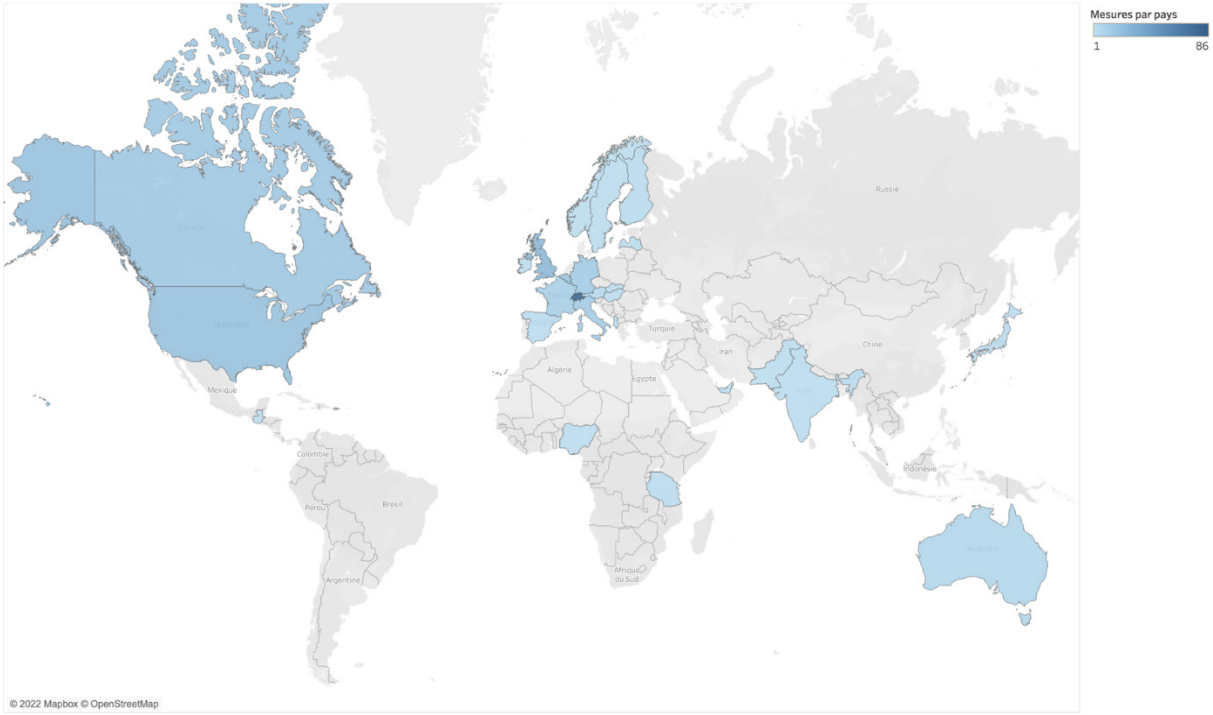
Après un bref aperçu des caractéristiques générales de l'ensemble des mesures détectées, nous décrivons plus en détails les mesures suisses, complétées par un regard sur la pratique observée dans d'autres pays.

4.3.1 Aperçu général des mesures en Suisse et ailleurs

L'étude a pu faire état de 257 mesures mises en place dans 29 pays différents (Fig. 2)[202]. Ces mesures sont récentes et la plupart sont encore en cours.

[201] Par exemple, discussion avec des collègues, médias, recherche libre.
[202] L'analyse documentaire – source principale de données pour les mesures étrangères – s'est concentrée uniquement autour de quatre langues (français, l'anglais, l'allemand et l'italien). Il paraît donc cohérent de voir principalement sur cette carte des pays ayant pour langue nationale au moins une de ces langues.

Fig. 2 – Carte du monde montrant la distribution des mesures recensées (n=243)*



* 14 mesures ont été mises en place par des organismes internationaux, tels que le Conseil de l'Europe ou Interpol : pour ces cas, aucun pays n'a été sélectionné.

L'on distingue parfois les mesures préventives des mesures répressives. Il ressort que la plupart des mesures détectées sont axées sur la prévention – sociale ou situationnelle –, étant donné qu'elles sont plus souvent rendues publiques que les mesures répressives ou d'enquête. Quant au public visé, nous relevons que les initiatives sont principalement développées à l'intention des enfants et des jeunes. Ce résultat s'explique en partie par la thématique spécifique de la présente étude.

La liste des mesures recensées peut être consultée dans l'annexe externe disponible en ligne, à la Section 3 (mesures suisses) et la Section 4 (mesures implémentées dans d'autres pays).

4.3.2 Les mesures existantes en Suisse et quelques exemples de la pratique d'autres pays

Au niveau suisse, l'étude a permis d'identifier 86 mesures. Nous les présentons dans les paragraphes suivants en trois blocs thématiques [203]:

- les mesures préventives ;
- les mesures techniques, et
- les mesures policières.

[203] Certaines mesures présentent des caractéristiques correspondant à plus d'un bloc thématique (par exemple, une mesure technique peut aussi être considérée comme une mesure préventive). Un choix d'attribution a été effectué, afin d'éviter de présenter une mesure à double et d'assurer une lecture fluide du rapport.

Pour chaque bloc, nous exposons les différents types d'activité (par ex. campagne, formation, brochure, etc.) en les illustrant à l'aide d'exemples concrets identifiés dans la pratique suisse. De plus, lorsque opportun, quelques exemples des mesures relevées dans d'autres pays sont présentés.

4.3.2.1 *Les mesures préventives*

Les mesures axées sur la prévention peuvent poursuivre plusieurs objectifs. Dans une perspective sociale, elles consistent, d'une part, à sensibiliser la population sur un phénomène et les risques associés et, d'autre part, à donner les outils nécessaires pour réagir en cas de nécessité. Tandis que, sous l'angle situationnel, les mesures implémentées contribuent à réduire les opportunités qu'un délit soit commis ou d'augmenter les chances que l'auteur soit découvert.

a) Campagne de sensibilisation à l'échelle nationale

Ce mode de prévention peut prendre des formes diverses, comme des spots publicitaires diffusés à la télévision ou sur les réseaux sociaux, des affiches dans la rue ou les écoles, ou encore des expositions temporaires. Les campagnes de sensibilisation sont souvent diffusées à large échelle (nationale, voire cantonale). En Suisse, une seule campagne de sensibilisation à l'échelle nationale a été détectée. Il s'agit de la campagne sur les cyber escroqueries « Et vous ? Vous auriez dit oui ? » déployée par les polices suisses en collaboration avec la PSC. Le cyber grooming et la sextorsion font partie de cette campagne. Dans ce cadre, des vidéos scénarisées mettant en scène des jeunes – auxquels les jeunes peuvent s'identifier – communiquant via leur smartphone avec ce qu'ils pensent être un autre jeune, alors qu'il s'agit en réalité d'un homme d'âge mûr. Cette campagne a été largement diffusée par les polices suisses, la PSC, les acteurs étatiques, et d'autres institutions.

Campagne nationale, quelques exemples de la pratique d'autres pays

- *Campagne de sensibilisation internationale* : la même campagne de sensibilisation peut également être diffusée dans plusieurs pays simultanément, comme la campagne « #DontBeAnEasyCatch »[204] sur le cyber grooming qui a été partagée dans 24 pays. Une telle démarche s'inscrit parfaitement dans le domaine de la prévention de la cybercriminalité dès lors que l'espace numérique ne connaît pas de frontière territoriale.
- *Journée nationale* : certains pays ont également des journées nationales dédiées à la prévention pour l'utilisation sûre des médias, où toutes sortes d'ateliers et d'activités sont mis en place dans les écoles. Par exemple, le Safer Internet Day – coordonné par le réseau INSAFE – est déployé dans près de 150 pays[205].

b) Informations et conseils

Une autre méthode consiste à mettre à disposition des informations, accompagnées de recommandations ou de conseils. Certaines institutions (gouvernements, associations, polices) mettent à disposition ces informations sur leur site Internet – consultation en ligne ou téléchargement de fichier PDF –, ou éditent des supports matériels (brochures, flyers, etc.).

[204] https://www.amberalert.eu/projects/dont-be-an-easy-catch
[205] https://www.saferinternet.fr/safer-internet-day/

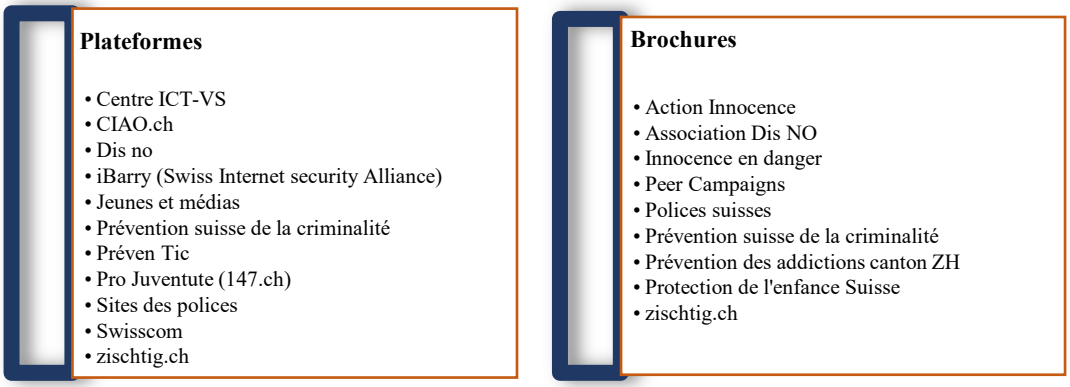
Plateformes en ligne : elles décrivent certains risques liés à Internet, tout en apportant des pistes sur le comportement à adopter lorsque l'on est confronté à un problème. La majorité des sites est destinée à un public large (par ex. PSC, sites des polices), alors que d'autres sont conçues spécifiquement à l'attention des enfants et des adolescents (par ex. CIAO.ch). Ces plateformes fournissent un réel effort pour être attrayantes pour cette population spécifique et les encourager à chercher des ressources plutôt que de se taire. Certaines plateformes prévoient également des ressources dédiées aux parents (par ex. Jeunes et médias, Pro Juventute).

Ce mode de prévention semble être le plus privilégié par les différentes institutions nationales et internationales, très certainement du fait de la facilité avec laquelle il peut être mis en place, son coût raisonnable face à d'autres activités, mais également la facilité d'accès pour des individus en quête de réponses, le tout anonymement et sans engagement.

Support matériel : cette formule apporte des informations condensées – parfois de celles qui peuvent être trouvées sur leur site Internet – afin que des enseignants les utilisent pour en parler pendant leur cours, que les parents les téléchargent afin d'aborder certains sujets avec leurs enfants, ou que les jeunes les consultent d'eux-mêmes.

En Suisse, plusieurs démarches similaires ont été identifiées. Par exemple :

Fig. 3 – Acteurs en Suisse mettant à disposition des renseignements sous format de plateformes ou de brochures



Informations et conseils, quelques exemples de la pratique d'autres pays

- *Bouton « Sortie »* : certains sites contiennent parfois un bouton « Sortie d'urgence » ou « Click to escape » visible sur toutes les pages du site pour ramener instantanément l'utilisateur à une page Internet neutre[206]. Cette fonctionnalité a pour but de pouvoir quitter rapidement la page Internet consultée et ainsi la victime ou l'auteur (potentiel) n'est pas surpris en train de chercher de l'aide. Cette méthode peut dès lors encourager les personnes à consulter plus librement ces plateformes d'informations et de conseils.
- *Guide sur les médias sociaux* : la plateforme en ligne ParentZone.org met à disposition des guides d'utilisation, à l'attention des parents, portant spécifiquement sur les réseaux sociaux, jeux vidéo en ligne ou autres plateformes largement fréquentés par les mineurs (Instagram, TikTok, Discord, Fortnite, etc.). Le guide apporte un grand nombre d'informations spécifiques au média sélectionné, tels qu'une description du contenu du média, des restrictions d'âge, des possibilités d'activation de fonctions de contrôle parental, des possibilités de dénoncer un comportement, etc.

c) Activités ludiques et éducatives

Cette catégorie inclut des mesures visant à alerter les enfants et les adolescents sur les dangers d'Internet de manière détournée et ludique, comme des livres, des sets de cartes, des jeux vidéo ou des capsules vidéo.

Livres et bandes dessinées : téléchargeables ou consultables sur Internet, ces supports sont un moyen d'aborder de manière ludique et détournée un sujet, avec comme protagoniste des enfants/adolescents ou des animaux. Deux initiatives ont été identifiées en Suisse. La Prévention suisse de la criminalité (PSC) a développé des livres audio – disponibles également en format texte – qui véhiculent des recommandations sur les dangers d'Internet dont la cyber grooming et la pédopornographie. Pour la seconde, il s'agit de courtes bandes dessinées « Les Websters » de l'OFCOM, disponibles en huit langues. Deux numéros mettent en scène une situation de cyber grooming.

Set de cartes : celui conçu par zischtig.ch, Curaviva (YOUVITA) et Santé sexuelle suisse, et soutenu par l'OFAS, permet d'aborder des sujets sur l'utilisation d'Internet en lien avec la sexualité, et plus particulièrement les services d'informations et de conseils en ligne, le cadre juridique, la pornographie, les rencontres en ligne, le sexting et les formes de chantage. D'autres initiatives de zischtig.ch et Curaviva (YOUVITA) ont été relevées, comme un set de cartes « Communication en ligne ».

Jeux : les activités ludiques et éducatives peuvent également prendre la forme d'un jeu, comme des quiz ou des jeux vidéo sérieux. Nous pouvons citer par exemple, le jeu Cyber Competizer[207], disponible en application ou site Internet, qui sensibilise les jeunes à la fraude, aux menaces techniques, à la protection des données, au cyberharcèlement ou au sexting à travers des fiches informatives et des quiz. En revanche, aucune initiative sur la thématique spécifique des cyber-délits sexuels n'a été identifiée en Suisse. Par contre, nous mentionnons aussi le projet pilote de jeu vidéo sérieux, mis en place par la Police cantonale vaudoise en 2014, portant sur la protection de l'image numérique des jeunes de 12 à 13 ans[208].

[206] Voir par exemple : https://www.stopitnow.org.uk/
[207] https://cybercompetizer.ch/#/login
[208] Petitpierre (2014).

Vidéos[209] : il peut s'agir de témoignages, de dessins-animés, ou de capsules vidéo de quelques minutes expliquant de manière succincte certaines thématiques et amenant des recommandations. Ces vidéos sont à libre disposition sur Internet pour une consultation personnelle ou pour être diffusées dans une salle de classe pour ouvrir la discussion. Par exemple, Pro Juventute a produit des vidéos d'environ une minute, notamment sur le cyber grooming et l'envoi de photos de nu[210]. Aussi, nous pouvons citer la web série « Teen Spirit » qui aborde le sexting et le revenge porn[211].

Activités ludiques et éducatives, quelques exemples de la pratique d'autres pays

- *Podcast* : en complément de vidéos, une police allemande a publié sur son site Internet un certain nombre de podcasts abordant différents types de cyber-délits sexuels (par ex. le cyber grooming)[212], à l'attention des adolescents.
- *Challenge TikTok* : AMBER Alert Belgique a mis en place une danse destinée à devenir virale, invitant de manière détournée les jeunes à reconnaître cinq signes indiquant qu'ils sont victimes de cyber grooming[213]. Cette démarche, unique, peut être un moyen original d'entrer en contact avec des jeunes en partageant les codes de ce réseau social.
- *Kit éducatif* : ce concept propose d'envoyer aux demandeurs des paquets contenant un certain nombre d'éléments destinés à être utilisés dans un cadre scolaire ou familial. Ils sont à disposition tout particulièrement des parents, des enseignants ou des professionnels en contact direct avec des jeunes afin d'aborder différents sujets liés à l'utilisation sécurisée des médias. Il s'agit en fait de donner aux demandeurs des outils adaptés et ludiques pour aborder des discussions avec des enfants ou des adolescents sans avoir recours à un formateur.
- *Jeu vidéo sérieux* : le Child Exploitation and Online Protection command de la National Crime Agency (Royaume-Uni) propose deux jeux interactifs, respectivement pour les enfants de 4 à 7 ans et de 8 à 10 ans[214]. Des situations s'affichent (par ex. un inconnu rencontré sur un jeu vidéo souhaite discuter en privé) et le joueur doit indiquer quel est le comportement à adopter (par ex. accepter l'invitation ou bloquer la personne). Un autre exemple de jeu vidéo sérieux pour les jeunes est celui en cours de développement au moment de la rédaction du rapport (juin 2022) par le projet RAYUELA (*Empowering and Education Young people for the Internet by playing*)[215]. Avec pour objectif de sensibiliser les jeunes aux bénéfices et aux risques d'Internet, plusieurs thématiques sont traitées dans des scénarios interactifs, dont le cyber grooming. En outre, le monitoring de ce jeu vidéo permettra d'établir les facteurs de risque de devenir victime d'un crime en ligne et améliorer les actions de prévention.

[209] Cette catégorie diffère des vidéos utilisées à des fins de sensibilisation dans le cadre des campagnes par le fait que (a) elles ne sont pas limitées à une diffusion pendant un temps donné et (b) elles ont une portée plutôt éducative pour compléter les informations présentes sur le site Internet, par exemple.
[210] https://www.projuventute.ch/fr/parents/medias-et-internet/videos-explicatives-medias-numeriques
[211] https://www.20min.ch/fr/story/decouvrez-les-episodes-de-teen-spirit-409936333495
[212] https://polizei.nrw/artikel/cyber-grooming
[213] https://www.checkbeforeyouchat.com/
[214] https://www.thinkuknow.co.uk/
[215] Projet financé par le programme de recherche et d'innovation H2020 de l'Union européenne. https://www.rayuela-h2020.eu/

d) Cours de sensibilisation ou formation

Des cours de sensibilisation ou des formations sont développés pour les enfants et les jeunes (en tant que victimes potentielles), et pour les adultes qui en ont la charge (enseignants, parents, professionnels), sous forme d'interventions en milieu scolaire, de conférences ou d'ateliers.

La majeure partie des formations est proposée par des organismes externes qui peuvent être sollicités afin de venir parler en classe à des enfants de tranches d'âge diverses, avec des contenus adaptés et plus ou moins ludiques. La plupart se concentre à expliquer aux enfants la « bonne » utilisation d'Internet, de la façon la plus sécurisée possible, en les alertant sur différents dangers et des mesures techniques à mettre en place (les mots de passe ou les filtres Internet, par exemple). Les formations proposées aux adolescents abordent plus en détails la sexualité (l'image de genre, la perception de son corps), certains comportements à caractère sexuel dont ils pourraient être victimes, ou les conséquences s'ils en étaient les auteurs. En ce sens, des informations en regard au droit en vigueur sont transmises afin de mettre en lumière ce qui est autorisé et ce qui ne l'est pas. Mais de manière générale, les cyber-délits sexuels semblent être abordés dans un cadre plus large des dangers d'Internet. Mentionnons toutefois un projet pilote lancé par Swisscom sur un module consacré aux contenus sexuels (l'image de genre, cyber grooming, sextorsion, etc.).

Le format (intervention théorique ou interactive), ainsi que le contenu exact de ces formations n'est pas connu. Nous soulignons en revanche une initiative de la Police neuchâteloise qui consiste à transmettre un numéro de téléphone aux jeunes pour qu'ils puissent contacter si besoin le chargé de prévention intervenu en classe, que ce soit par téléphone ou par message.

Les formations – sous forme de soirée d'information, conférence ou atelier – s'adressent également aux personnes qui pourraient être en contact avec les jeunes, comme les parents ou les enseignants, pour apprendre « la meilleure façon d'apprendre » et transmettre les mêmes messages qu'aux jeunes. Le discours s'oriente aussi parfois sur les raisons pour un jeune d'être en ligne et comment cela s'inscrit dans le processus de socialisation. D'autres aspects de ces mesures portent également sur comment réagir lorsqu'on se trouve dans une situation inconnue ou comment chercher le dialogue avec l'enfant ou l'adolescent, sachant que ce qui a trait à la sexualité demeure parfois un sujet tabou.

En Suisse, plusieurs institutions ont développé des formations ou cours de prévention (*supra*, ch. 4.2.1).

Formations, quelques exemples de la pratique d'autres pays

- *Séminaire* : nous avons également pu trouver certains séminaires qui s'adressaient à des professionnels très spécifiques, comme les agents de police ou les juristes, afin de les sensibiliser à la manière dont ces sujets, parfois sensibles pour les victimes, devraient être abordés.

e) Aide et soutien (avec ou sans option de traitement)

Ce volet se réfère aux mesures visant à apporter de l'aide et du soutien aux victimes et à leur entourage, ainsi qu'aux (potentiels) auteurs et à leurs proches. Cette assistance peut se matérialiser sous diverses formes : permanence d'aide et/ou conseils, service de conseils juridiques, thérapies.

Service de permanence : les centres cantonaux LAVI sont les structures principales d'aide aux victimes d'infraction et fournissent une aide psychologique, juridique, sociale et matérielle aux victimes[216]. Les centres peuvent être contactés par téléphone ou par courriel électronique. Au-delà de ces structures étatiques, certaines institutions (ex. Pro Juventute) gèrent et proposent directement via leur site Internet un service de permanence via différents canaux de communication (téléphone, e-mail, chat)[217]. Alors que des services sont dédiés aux victimes et à leur entourage, d'autres structures – Association Dis NO, Beforemore, Io No![218], et Kein Täter Werden – proposent ce service aux (potentiels) auteurs, ainsi qu'à leurs proches et aux éventuels témoins (par exemple, des personnes tombant sur des images pédopornographiques). Selon la situation et les besoins exprimés par la personne, celle-ci sera orientée vers un service spécialisé.

Conseils juridiques : cette activité propose une aide juridique aux enfants victimes. Lorsque les victimes sentent le besoin d'avoir l'appui d'un avocat, que ce soit pour des démarches juridiques, des demandes de conseils liées à un événement ou une plainte, elles peuvent faire appel à certaines institutions.

Dans cette perspective, les Centres cantonaux d'aide aux victimes LAVI offrent des conseils juridiques aux victimes, mettent à disposition un avocat et peuvent accompagner la victime tout au long d'une procédure pénale. Si besoin, la victime est orientée vers un autre service[219].

En Suisse romande, un enfant peut aussi contacter gratuitement – par téléphone du lundi au vendredi (9h-17h) – un avocat de la permanence Juris Conseil Junior. Aucun domaine spécifique de compétence n'est indiqué. Néanmoins, dès lors que Juris Conseil Junior travaille en étroite collaboration avec CIAO.ch, nous pouvons supposer que la permanence peut intervenir dans les situations de cyberdélinquance sexuelle.

Thérapies psychologiques[220] : cette activité peut être proposée tant pour une population qui aurait déjà été victime ou ayant commis un cyber-délit sexuel envers un mineur, que pour des personnes se sachant attirées par des enfants mais n'étant pas passées à l'acte.

En matière de prévention secondaire, un rapport du Conseil fédéral de septembre 2020 – en réponse aux postulats Rickli 16.3637 et Jositsch 16.3644 et s'appuyant sur un rapport de recherche mandaté à cette fin[221] – avait souligné que « la Suisse ne dispose pas d'une offre de traitement spécialisée, structurée et incluant toutes les régions linguistiques destinée aux personnes attirées sexuellement par les enfants »[222,223]. En effet, les quatre offres existantes jusque-là consistaient plutôt en des initiatives individuelles et réservées aux personnes ayant déjà commis une infraction sexuelle[224]. En parlant plus

[216] https://www.aide-aux-victimes.ch/fr/ou-puis-je-trouver-de-laide/
[217] En complément de l'espace de discussion avec un conseiller ou une conseillère, 147.ch de Pro Juventute offre également la possibilité de chatter avec des jeunes du même âge.
[218] Ces informations se fondent sur les données récoltées entre décembre 2021 et mai 2022. L'association Io No! sera prochainement rattachée à l'association Dis No.
[219] https://www.aide-aux-victimes.ch/fr/ou-puis-je-trouver-de-laide/
[220] Il se peut que des mesures d'aide thérapeutiques n'aient pas été détectées, car elles se focalisent rarement sur un comportement spécifique, mais couvrent plutôt des thématiques plus larges, telles que les attirances sexuelles ou la violence sexuelle.
[221] Niehaus, Pisoni, et Schmidt (2020).
[222] Conseil fédéral (2020a, p. 27).
[223] Le rapport du Conseil fédéral (2020a) mentionne également que « les offres existantes sont des initiatives individuelles et, à l'exception des services offerts par FORIO [Institut des sciences criminelles de Suisse orientale], les offres de traitement sont peu spécifiques ou difficilement trouvables en ligne, car les prestataires ne sont pas systématiquement mis en réseau » (p. 27-28).
[224] Niehaus et al. (2020).

spécifiquement des personnes attirées sexuellement par les enfants et les adolescents, le rapport de recherche relèvent que celles-ci ne sollicitent pas les services de soutien notamment en raison du manque de connaissances quant à ces offres et de la distance géographique entre le domicile et le service de soutien[225] (expliquée en partie par l'insuffisance de ces services).

Depuis lors, une nouvelle infrastructure s'est implémentée en Suisse. Il s'agit de Kein Täter Werden, un projet originaire d'Allemagne. Toutefois, encore en développement, l'offre reste principalement concentrée en Suisse allemande (à l'exception de Genève). Par ailleurs, le site Internet est pour le moment uniquement disponible en allemand.

Une aide thérapeutique peut également être obtenue de manière indirecte en passant par les associations susmentionnées (Dis No, Beforemore, Io No ![226]) qui ont formé un réseau de thérapeutes expérimentés. Elles ne proposent pas directement des options de traitement mais peuvent rediriger les personnes sollicitant une telle aide vers des spécialistes.

Aide et soutien (avec ou sans option de traitement), quelques exemples de la pratique d'autres pays

- *Groupe de soutien* : une institution canadienne a mis en place des groupes de soutien qui offrent la possibilité aux victimes de cyber-délits sexuels – de catégories d'âge diverses – de se réunir[227]. Un groupe de soutien est d'ailleurs spécifiquement dédié aux victimes qui ont des images pédopornographiques les représentant toujours en circulation sur les réseaux pédophiles.
- *Centre spécialisé* : deux services de conseils juridiques pour enfants ont été identifiés aux Etats-Unis, l'un dans un centre de défense pour enfants[228], l'autre dans un centre de prévention des abus à l'encontre des enfants[229].
- *Service d'entretien médico-légal* : ce service, mis en place par Alliance for Children (organisation américaine à but non lucratif), propose de mener des entretiens avec des enfants victimes d'abus sexuels, afin de « de recueillir des informations pertinentes auprès des enfants d'une manière neutre, non suggestive et légalement défendable »[230]. Nous ne sommes pas en mesure de préciser si ce service est aussi destiné à des victimes de cyber-délit.
- *Avatar sur jeu vidéo* : pendant la période de confinement en 2020 due à la pandémie du Coronavirus, l'association Enfant bleu, en collaboration avec la Police nationale française, a installé un avatar sur le jeu vidéo Fortnite. Cette initiative, visant à détecter les violences à l'encontre des mineurs, permettait à un enfant se sentant en danger de le signaler en direct. La publicité autour de cette initiative s'est faite via les réseaux sociaux (dont Snapchat et Instagram), ainsi que par le biais d'influenceurs reconnus dans le monde des jeux vidéo. Un groupe de travail a été formé en vue de pérenniser la démarche[231].

[225] Niehaus et al. (2020).
[226] Ces informations se fondent sur les données récoltées entre décembre 2021 et mai 2022. L'association Io No! sera prochainement rattachée à l'association Dis No.
[227] https://protectchildren.ca/en/programs-and-initiatives/survivor-advocacy-groups/
[228] https://www.allianceforchildren.org/what-we-do
[229] http://www.thecapcenter.org/
[230] https://www.allianceforchildren.org/mission-history
[231] https://enfantbleu.org/operation-lenfant-bleu-sur-fortnite-quand-le-jeu-video-peut-aider-a-sauver-des-vies/

4.3.2.2 *Les mesures techniques*

Cette catégorie englobe des dispositifs ou programmes destinés principalement à être appliqués sur des appareils numériques, tels que les ordinateurs ou les smartphones, ou des sites Internet. Relevant de la prévention situationnelle ou de la répression, ces mesures permettent soit de réduire les opportunités ou les risques qu'un délit soit commis, soit à découvrir plus facilement la commission d'un délit.

Une majorité de ces programmes ont pour vocation de détecter les images à caractère pédopornographique et soit à les bloquer directement, soit à envoyer une alerte vers l'appareil pour prévenir l'individu qu'il s'apprête à commettre une infraction pénale s'il poursuivait. Ils sont développés par (a) des multinationales commercialisant des appareils numériques, (b) des gouvernements ou des organismes internationaux qui visent la mise en place de mesures à une large échelle, et (c) des fondations ou entreprises indépendantes.

a) Logiciels de contrôle et de blocage

Cette première catégorie inclut les logiciels de contrôle et de blocage pouvant être utilisés par quiconque. Les parents recourent à ce type de technologie pour sécuriser les appareils numériques utilisés par les enfants. D'autre part, les établissements scolaires font aussi usage de tels logiciels afin de protéger les élèves lorsqu'ils utilisent le matériel informatique de l'école (contrôle parental, pare feu).

Les services de télécommunication suisses, comme Swisscom (Internet Security) ou Sunrise (Kapersky Safe Kids), proposent des fonctionnalités ou des logiciels de contrôle parental permettant de bloquer l'accès aux sites indésirables ou dangereux, de limiter l'accès à certains types de contenus, et à certaines pages Internet.

Pro Juventute propose également une application de contrôle (Wup) qui détecte, sur les médias sociaux et les messageries instantanées utilisés par le mineur, les photos de nudité, le harcèlement, et le partage de données personnelles. Lorsque l'application détecte un tel contenu, elle affiche une information ou un conseil pour le mineur.

Des entreprises commercialisant des services technologiques ou des appareils numériques, comme Google et Apple, proposent également une fonction pour pouvoir restreindre l'accès à des applications, des fonctionnalités ou à des contenus spécifiques (comme le contenu pédopornographique).

Au-delà de la détection d'images, d'autres logiciels ont pour fonction d'analyser les textes des conversations, et ceci afin de lutter contre le cyber grooming. Par exemple, Microsoft a lancé le projet Artemis en 2020[232].

Logiciels de contrôle et de blocage, quelques exemples de la pratique d'autres pays

Deux autres types de logiciels détectés à l'étranger peuvent être inclus dans cette catégorie.

- *Détection d'images pédopornographiques connues :* des outils visent à détecter des images à caractère sexuel sur des sites Internet préalablement signalés. La plateforme Arachnide, lancée par le Centre canadien de protection de l'enfance (CCPE) en 2017, permet d'identifier de telles

[232] Dans la même idée, nous pouvons citer l'application SafeToNet pour smartphone qui analyse les discussions et identifie tout élément pouvant indiquer une situation dangereuse (https://safetonet.com).

images en se fondant sur deux bases de données d'images connues[233]. À la suite d'une détection, une demande de suppression est envoyée à l'hébergeur. Le CCPE a également développé « Shield par Projet Arachnide » destiné aux entreprises afin de détecter des images pédopornographiques sur leur serveur.

- *Blocage de téléchargements* : des programmes et/ou des applications ont été développés pour empêcher le téléchargement de contenu pédopornographique. Par exemple, la Fondation Prostasia propose une telle application en téléchargement libre sur son site Internet[234].

Notons que certaines mesures techniques, bien que communiquées sur des sites non-suisses, peuvent tout à fait être téléchargées et appliquées à des appareils électroniques suisses.

b) Logiciels de détection

D'autres logiciels intègrent des technologies plus avancées et se destinent à un public plus spécifique tels que les autorités policières ou des ONG œuvrant dans la lutte contre la pédocriminalité. L'analyse documentaire n'a pas permis d'identifier ce type de mesure en Suisse, et très peu de résultats à l'étranger[235].

Logiciels de détection, quelques exemples de la pratique d'autres pays

Deux types de logiciels détectés à l'étranger peuvent être inclus dans cette catégorie.

- *Enfant modélisée* : une enfant modélisée en 3D a été utilisée dans le but d'appâter les amateurs de live-streaming afin de pouvoir les poursuivre pénalement [236]. Le software, appelé Sweetie 2.0, a été développé par Terre des hommes.
- *Reconnaissance faciale et audio :* les logiciels intégrant des méthodes de détection basées sur la reconnaissance visuelle ou audio peuvent poursuivre plusieurs objectifs. Par exemple, le logiciel Biometric Analyser and Network Extractor (BANE), en cours de développement en Australie, se fonde sur la reconnaissance de données biométriques afin de détecter et relier des victimes d'abus sexuel. Alors que l'outil Yoti utilise la reconnaissance faciale pour estimer l'âge d'un mineur[237]. Cette technique – utilisée notamment par Meta – peut servir comme vérificateur d'âge pour les plateformes en ligne.

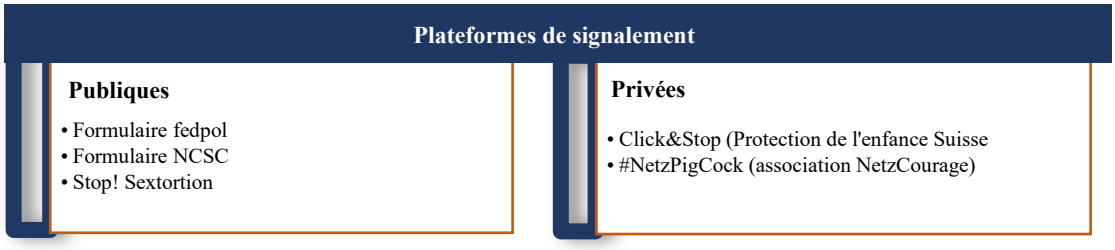
[233] https://projetarachnid.ca/fr/
[234] https://prostasia.org/fr/project/csam-scanning-plugins/
[235] Nous recommandons une recherche complémentaire portant spécifiquement sur les nouvelles techniques de détection. Sur la base des entretiens, il ressort qu'un grand nombre de projets sont en cours de développement mais qu'il peut s'avérer complexe d'avoir une vue d'ensemble sur ceux-ci, dès lors qu'ils sont parfois gardés confidentiels.
[236] https://www.terredeshommes.nl/en/programs/sweetie
[237] https://www.yoti.com/

c) Plateformes de signalement

Ce type d'outil offre à la population la possibilité de signaler une infraction dont elle a été victime ou la découverte d'un matériel de pornographie interdite – y compris la pornographie enfantine – sur Internet. Pour cette dernière, selon le pays, seul l'URL menant audit matériel est transmis afin de ne pas se rendre coupable soi-même de possession de pornographie. Ces plateformes peuvent être gérées directement par les autorités policières, ou indirectement par une institution – habilitée à recevoir ce type de contenu illicite – qui se chargera ensuite, soit de transmettre directement les informations à l'autorité compétente, soit de procéder à un premier triage du contenu et ensuite rediriger le dossier.

En Suisse, plusieurs plateformes de signalement ont été identifiées. Celles-ci permettent uniquement l'envoi de liens URL, le triage du contenu étant par la suite effectué par fedpol.

Fig. 4 – Plateformes de signalement recensées en Suisse



Les autorités étatiques proposent trois moyens de signalement se distinguant sur le contenu de la dénonciation. Alors que le formulaire de fedpol est réservé à la dénonciation de matériel de pornographie interdite, celui du NCSC[238] couvre l'ensemble des délits cyber, ce qui inclut la sextorsion, le cyber grooming et le live-streaming. Quant au troisième, l'initiative Stop ! Sextorsion concerne spécifiquement les emails de sextorsion où un versement (généralement en bitcoin) est réclamé. Via cette plateforme, les emails peuvent être transmis aux autorités afin de les aider dans leurs enquêtes. Bien évidemment, ces plateformes viennent en complément de la voie plus traditionnelle qui consiste à notifier ou déposer une plainte auprès des postes de police ou du ministère public.

Deux autres initiatives proviennent d'associations actives dans le domaine de la protection des enfants et des jeunes contre la délinquance sexuelle en ligne. Le formulaire #NetzPigCock de l'association NetzCourage est une plateforme de signalement d'envoi de contenus pornographiques non sollicités, ainsi qu'un service d'accompagnement pour le dépôt de plainte. Quant à la deuxième initiative, il s'agit du formulaire Click&Stop[239]– lancé en 2022 par la Protection de l'enfance Suisse et l'association Guido Fluri –, qui est un service de signalement en ligne contre la violence sexuelle envers les enfants et les adolescents.

[238] Le NCSC récolte les liens dénoncés et transmet directement à fedpol, sans trier ni ouvrir les contenus.
[239] Click&Stop récolte les liens dénoncés et transmet directement à fedpol, sans trier ni ouvrir les contenus.

d) Charte de sécurité

Les chartes de sécurité sont un document rappelant les règles de bonne conduite à un groupe de personnes. Elles permettent de rappeler que certains comportements ne sont pas tolérés (par exemple, le harcèlement ou l'échange/la consultation de matériel pornographique), et peuvent même être criminalisés par le droit en vigueur. Bien que les quatre phénomènes d'intérêt ne soient pas toujours explicitement mentionnés, de telles chartes sensibilisent les signataires à la bonne utilisation des outils technologiques, ainsi qu'à la problématique de la violence sexuelle en ligne et aux dynamiques d'intimidation sexuelle.

En Suisse, certaines écoles établissent une charte de sécurité qui doit être obligatoirement signée par les élèves, ou par les élèves et les parents.

e) Banque de mèmes

Cette démarche aborde le sujet du sexting et de la sextorsion de façon amusante. Elle a pour but de fournir des mèmes à envoyer aux demandeurs insistant d'images de nus, servant ainsi de réponse toute prête aux jeunes ne sachant comment refuser.

Aucune initiative similaire n'a été identifiée en Suisse sur la thématique de la criminalité sexuelle en ligne. En revanche, dans le même esprit, Swisscom a créé des mèmes dans le cadre de son initiative « Mute the hate » pour lutter contre les discours haineux en ligne.

Banque de mèmes, un exemple de la pratique d'autres pays

- Au Canada, une banque de mèmes de rat-taupe nu est disponible[240].

4.3.2.3 *Les mesures policières*

Dans cette section dédiée aux mesures policières, sont présentés certains outils et méthodes de travail de la police[241]. En effet, certains moyens d'investigation ne peuvent pas être publiquement divulgués afin d'assurer la bonne continuité du travail des forces de l'ordre. Sans entrer dans les détails opérationnels, nous exposons brièvement six outils ou méthodes de travail – mis en évidence par la présente étude – contribuant à la prévention et à la lutte contre la délinquance sexuelle en ligne à l'encontre des mineurs.

- *Suivi des annonces NCMEC* : plusieurs pays, dont la Suisse, collaborent étroitement avec l'organisation américaine National Center for Missing & Exploited Children (NCMEC) qui envoie des annonces, provenant notamment de fournisseurs de services de télécommunication américains, qui ont un lien réel ou supposé avec la Suisse. Fedpol effectue une première analyse, d'une part, quant à la nature illicite en regard du droit pénal suisse et, d'autre part, sur l'identification de l'expéditeur du contenu. Le dossier est ensuite transmis au canton concerné en vue d'investigations ultérieures et/ou de l'ouverture d'une procédure pénale.

[240] https://dontgetsextorted.ca/
[241] Les informations présentées dans cette section sont issues des entretiens menés avec des corps de police suisses.

- *Monitoring des téléchargements illicites* : la police peut traquer les téléchargements peer-to-peer grâce au logiciel américain CPS. Le logiciel analyse les valeurs hash associées à une image. Cette veille vise les contenus échangés entre privés, et non les images hébergées sur des sites Internet.
- *Blocage de site Internet* : lorsqu'elle reçoit un signalement, la police est habilitée à bloquer une page Internet. Elle informe ensuite le fournisseur de services ou le partenaire étranger.
- *Recherches secrètes préventives (ou infiltration)* : un enquêteur infiltre un réseau social ou un chat avec un profil faisant croire qu'il s'agit d'un mineur. Dans un premier temps, il s'agit d'une démarche passive dès lors que l'enquêteur va attendre que des personnes initient le contact. Si une rencontre à des fins sexuelles est proposée, la police organise l'interpellation du pédocriminel. La police possède une liste de sites connus pour ce type de pratique.
- *Base de données de police nationale et internationale* : les contenus pédopornographiques détectés par la police peuvent ensuite être confrontés à la base de données nationale et, au niveau international, à la base de données ICSE (Internet Child Sexual Exploitation) de Interpol. Si le contenu est connu, des informations complémentaires peuvent être consultées. Notamment un code couleur permet de remonter à l'identité de la victime et/ou de l'auteur. Un espace discussion est à disposition des policiers pour l'échange d'informations (par exemple, si un policier reconnaît un agresseur ou un élément de décor).
- *Collaborations* : l'échanges avec d'autres autorités policières/judiciaires ou ONG, au niveau national et international, est primordial. La collaboration avec NCMEC est un premier exemple. Un second est la collaboration entre le centre régional de compétence en cybercriminalité (RC3) de Genève et le ministère public de Manhattan sur l'achat de matériel pédopornographie à l'aide de cryptomonnaie.

4.3.2.4 *Caractéristiques des mesures existantes en Suisse*

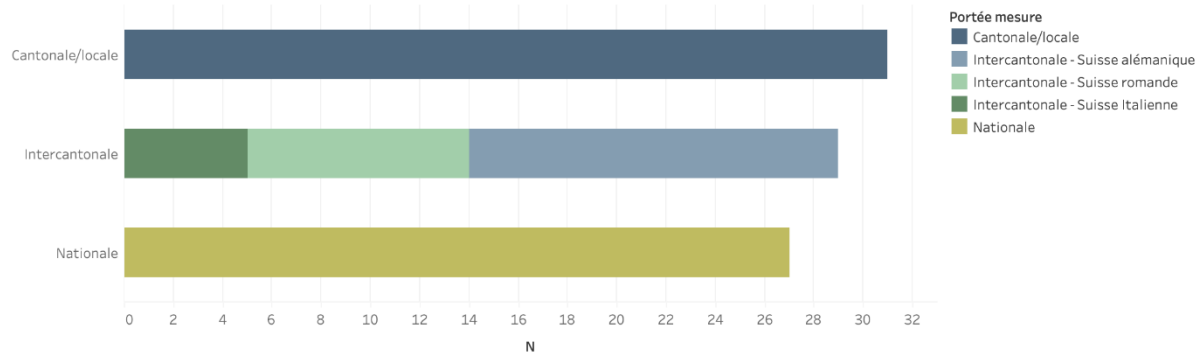
Dans cette section, nous apportons une vue générale sur l'ensemble des mesures identifiées en Suisse[242]. En ce sens, un éclairage spécifique est posé sur la portée géographique des initiatives, le format adopté, le public cible, ainsi que les phénomènes adressés.

a) Portée géographique des mesures

La figure 5 montre que plus de la moitié des mesures identifiées sont implémentées ou rendues accessibles à une échelle cantonale, voire locale. Les mesures développées dans une perspective nationale représentent un peu plus d'un quart des mesures identifiées. Enfin, d'autres mesures trouvent une portée plus régionale. Conforme à la répartition régionale de la Suisse, les mesures disponibles en Suisse alémanique sont plus nombreuses que les mesures conçues pour la Romandie ou la Suisse italienne.

[242] Pour cette section 4.3.2.4, les mesures policières explicitées en amont ne sont pas incluses, car s'agissant davantage de méthodes et outils de travail utilisés par les corps de police, il n'est pas possible de les quantifier.

Fig. 5 – Distribution des mesures suisses selon leur portée géographique*

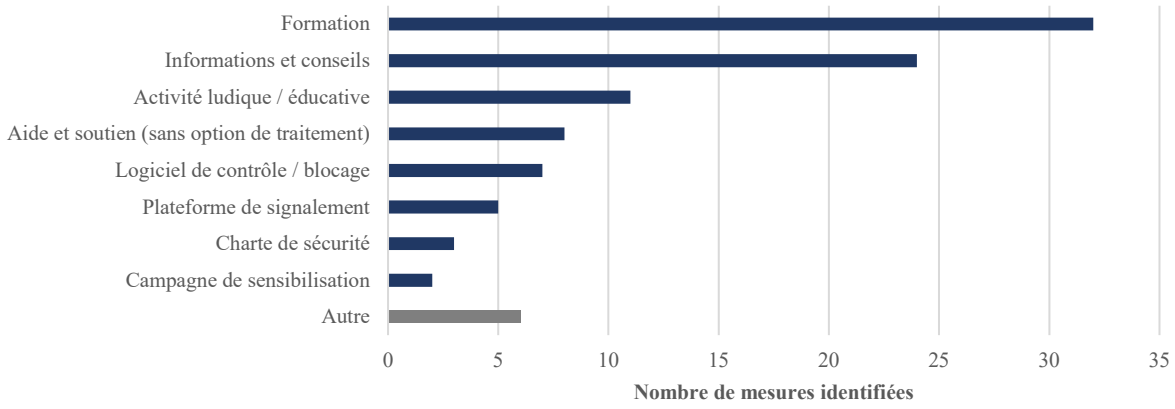


* Le graphique se fonde sur 81 mesures. Pour cinq mesures, il n'a pas été possible de déterminer la portée géographique.

b) Format des mesures

En regard au format adopté, nous relevons que les efforts sont majoritairement concentrés sur la formation (Fig. 6). Il s'agit principalement des cours de sensibilisation dispensés en milieu scolaire. Le second type de mesure le plus fréquent est la diffusion d'informations et de conseils. Suivent ensuite les activités ludiques et éducatives, et d'aide et soutien (sans option de traitement). Enfin, la campagne de sensibilisation est la catégorie de mesures la moins fréquente.

Fig. 6 – Distribution des mesures suisses selon le format adopté*



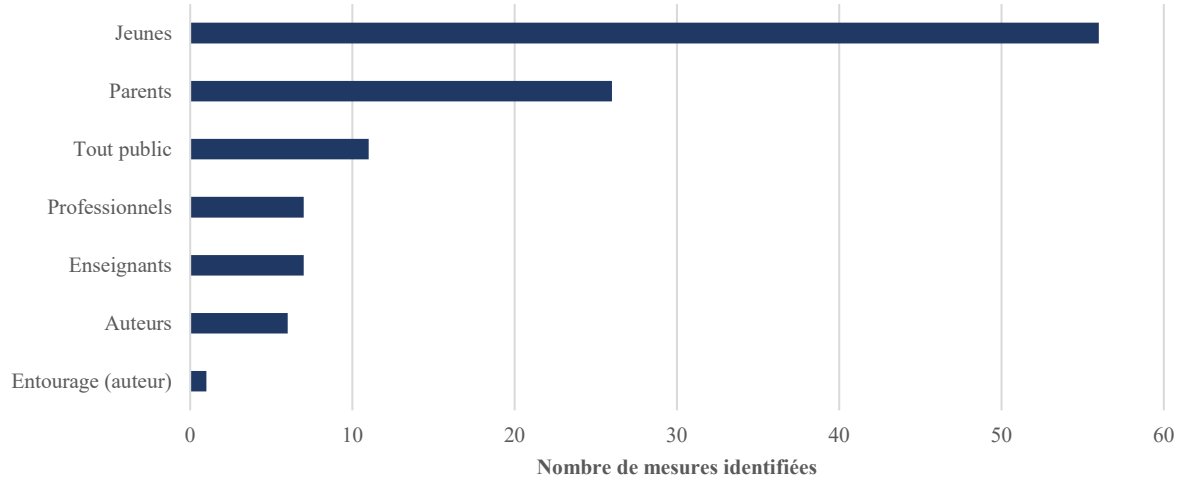
* Le graphique se fonde sur 86 mesures. Cependant, une initiative peut être déployée sous plusieurs formes, ce qui explique que le nombre total soit plus grand dans ce graphique.

Note. La catégorie « autre » comprend deux études scientifiques menées sur la thématique et 4 manifestations.

c) Public ciblé par les mesures

Une mesure peut être adressée à toute la population ou alors s'intéresser expressément à un groupe ou des groupes spécifiques. La figure 7 ci-dessous montre que presque la moitié des mesures sont destinées aux jeunes, ce qui s'explique du fait de la thématique investiguée. Suivent ensuite les mesures adressées aux parents. Comme nous l'avons vu précédemment, plusieurs mesures prévoient un volet consacré aux parents afin de leur transmettre les mêmes messages qui sont véhiculés aux jeunes, ainsi que de leur donner les outils pour accompagner les mineurs. En revanche, nous relevons que peu d'initiatives sont formulées pour les enseignants et autres professionnels travaillant avec des enfants et des adolescents.

Fig. 7 – Distribution des mesures suisses selon le public cible*



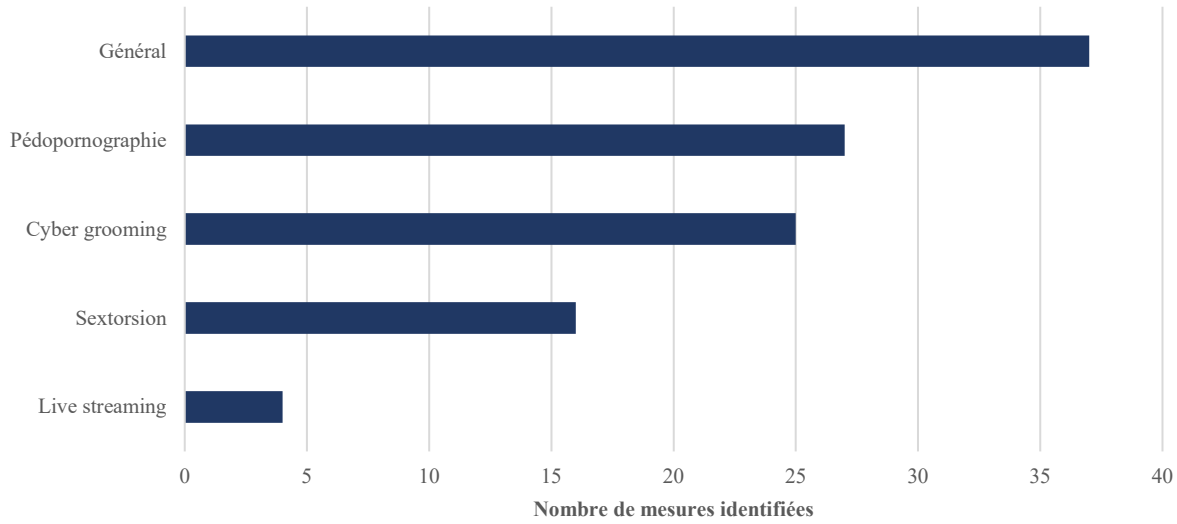
* Le graphique se fonde sur 86 mesures. Cependant, une initiative peut cibler plusieurs publics, ce qui explique que le nombre total soit plus grand dans ce graphique.

d) Phénomènes adressés par les mesures

La figure 8 indique la distribution des mesures suisses selon leur contenu en lien avec les quatre phénomènes. Une grande prudence est requise dans l'interprétation des résultats dès lors que le contenu des initiatives n'est pas disponible pour toutes les mesures, et le niveau de détails varient fortement entre les mesures. Alors que pour certaines mesures, les types de cyber-délits sont explicitement mentionnés, pour d'autres l'information est plus floue.

Nous pouvons toutefois relever quelques observations intéressantes. Tout d'abord, un grand nombre de mesures tendent à rester à un niveau plus général de bonnes pratiques en termes d'utilisation des médias et des risques inhérents, dont les délits sexuels. D'autre part, nous relevons que l'attention se porte davantage sur la pédopornographie et le cyber grooming que sur la sextorsion. Enfin, il ressort également que le live-streaming est peu abordé dans les mesures. Ceci concorde avec les résultats de la littérature scientifique, où nous avons constaté un faible nombre d'études réalisées sur le sujet.

Fig. 8 – Distribution des mesures suisses selon leur contenu en lien avec les quatre phénomènes*



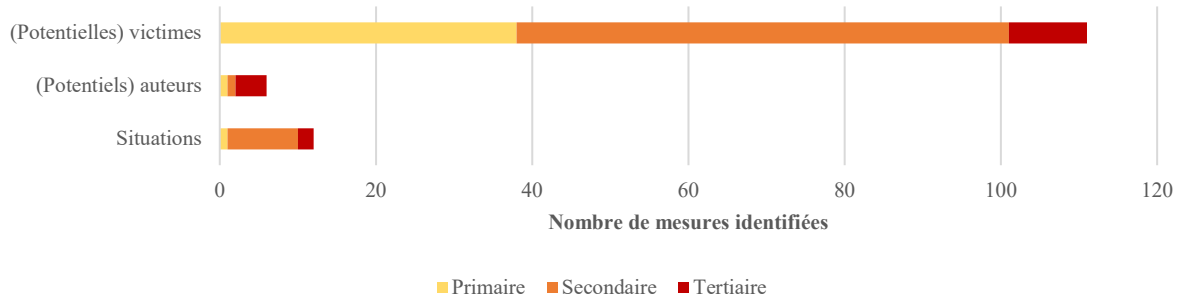
* Le graphique se fonde sur 86 mesures. Cependant, une initiative peut aborder plusieurs sujets, ce qui explique que le nombre de mesures soit plus grand dans ce graphique.

e) Types de prévention visés par les mesures

Pour terminer, nous passons en revue les types de mesures mises en place selon la classification de van Dijk et de Waard (1991) qui combine les types de prévention avec leur cible (Fig. 9).

Comme nous pouvons le constater, les mesures s'adressant aux (potentielles) victimes représentent la majorité. Les mesures qui tendent à modifier l'environnement – situations – et les mesures destinées aux (potentiels) auteurs sont plus rares. De plus, les mesures se fondent principalement sur la prévention secondaire, avec des mesures destinées aux jeunes. Un certain nombre de mesures relevant de la prévention primaire visent plutôt des mesures pour les parents et les professionnels. Les mesures adressées à la population générale sont limitées. Enfin, nous relevons une lacune dans le domaine de la prévention tertiaire.

Fig. 9 – Distribution des mesures suisses selon le type de prévention et la cible*



* Le graphique se fonde sur 86 mesures. Cependant, une initiative peut poursuivre plusieurs types de prévention et de public, ce qui explique que le nombre de mesures soit plus grand dans ce graphique.

4.3.3 Applicabilité en Suisse des mesures identifiées dans d'autre pays

Dans les sections précédentes, nous avons exposé plusieurs exemples de pratiques identifiées dans d'autres pays. Il convient de préciser que ces initiatives ne doivent pas être considérées comme des modèles de bonnes pratiques absolues, mais plutôt comme des mesures dont les acteurs suisses peuvent s'inspirer. En effet, l'étude actuelle ne permet pas de déterminer si ces initiatives sont efficaces et dans quelle mesure elles sont applicables en Suisse. Les raisons principales sont les suivantes :

- *Informations partielles sur l'implémentation des initiatives* : le concept d'une mesure est souvent décrit de manière générale, en exposant les grandes lignes de celle-ci. Ainsi, sans disposer des informations de détails sur leur implémentation, il est difficile de reproduire la même action.
- *Efficacité des mesures inconnue* : même si une multitude d'initiatives ont été mises en place, peu d'entre elles ont fait l'objet d'une évaluation rigoureuse pour en connaître l'efficacité. C'est un constat général que l'on peut faire sur les programmes de prévention, et encore plus en lien avec la cybercriminalité qui est un phénomène relativement récent[243]. Pour cette raison, il est difficile d'établir des bonnes pratiques en la matière.
- *Transposabilité des mesures dans un nouvel environnement* : la plupart des mesures, ou des études scientifiques, ne peuvent pas être transposées dans leur intégralité dans un nouvel environnement avec l'assurance d'obtenir des résultats identiques. En effet, les initiatives doivent être adaptées aux spécificités du lieu d'implémentation, que ce soit en termes de contexte social ou des caractéristiques du phénomène criminel que l'initiative vise. Il est donc pertinent d'avoir une connaissance fine tant des paramètres d'implémentation de la mesure dans le pays d'origine que du contexte du nouvel environnement où la mesure doit être répliquée.

Ainsi, les exemples de pratiques identifiées dans d'autres pays peuvent uniquement fournir des pistes de réflexion pour élaborer de nouvelles mesures en Suisse ou remanier des mesures existantes. Un tableau de synthèse est proposé au chapitre 5.

4.4 Les avis des experts sur les initiatives entreprises en Suisse et ailleurs

Les échanges avec des experts (ci-après: les experts interviewés ou les interviewés) venant de Suisse et d'ailleurs ont été très bien accueillis, du fait de l'importance du sujet reconnue à l'échelle internationale. Les entretiens ont permis d'aborder des perspectives complémentaires sur la thématique des cyber-délits sexuels à l'encontre des mineurs.

De manière générale et à l'image des résultats présentés dans les sections précédentes, l'exploitation de mineurs par le biais de matériel pédopornographique sous l'angle de la diffusion de matériel[244] ou du cyber grooming sont les deux phénomènes les mieux connus par les experts interviewés, suivi par la sextorsion. En revanche, nous observons que le live-streaming, bien que l'on en entende de plus en

[243] Pour plus de détails, voir Brewer et al. (2019).
[244] Le matériel pédopornographique est rarement produit en Suisse.

plus parler, ce phénomène semble encore passablement méconnu. Seuls les experts interviewés du milieu policier ou du milieu technique ont pu partager leurs opinions à ce sujet.

Les éléments relevés dans le cadre de ces entretiens sont présentés en quatre thématiques :

- les cyber-délits à l'encontre des mineurs,
- les politiques de prévention et de soutien,
- les politiques de répression, et
- les perspectives futures.

Dans les sections suivantes, il sera fait référence aux experts interviewés au moyen de pseudonymes sur la base de la matrice suivante :

Tab. 12 – Matrice de référencement des interviewés

Domaine d'activité	Pseudonymes
Police	Pol-1 à Pol-7
Prévention sociale	PrévSo-1 à PrévSo-7
Prévention situation	PrévSit-1
Justice	Juris-1 à Juris-3

4.4.1 Les cyber-délits sexuels : tendances et caractéristiques

L'état des lieux, en termes d'ampleur et d'évolution, était habituellement l'une des premières thématiques approfondies dans les entretiens. Le constat général, partagé par la plupart des interviewés, est que l'omniprésence des outils numériques dans la société d'aujourd'hui contribue à l'accélération de certains phénomènes réalisés en ligne, dont les délits sexuels à l'encontre des mineurs. Le discours des experts interviewés tournait principalement autour de trois arguments.

Tout d'abord, les avancées technologiques offrent des moyens et opportunités supplémentaires pour commettre des actions malveillantes, qui sont perfectionnés au fil du temps. Alors qu'avant un prédateur allait roder près des écoles ou des places de jeux, aujourd'hui il peut entrer en contact avec des mineurs en restant derrière un écran. De plus, les modes de communication et d'échanges ont évolué en passant du simple message textuel à l'envoi de photo, suivi de vidéo, et maintenant à la réalisation de vidéo en directe. En matière de distribution de contenus illicites, les capacités d'échange ont aussi progressé passant de l'envoi de quelques images – en raison d'un faible débit – au transfert de centaines d'images et/ou de vidéos. Selon l'un des experts interviewés, Internet fonctionne comme un catalyseur en permettant aux pédocriminels de se regrouper, d'échanger. L'effet de groupe peut aussi potentiellement pousser un individu à réaliser des actions plus vite, qu'il n'aurait pas commis sans l'influence des pairs.

Ensuite, les experts interviewés relèvent que les mineurs ont un accès à des appareils numériques et à Internet dès un très jeune âge (avant 10 ans). D'une part, les ordinateurs et les tablettes font leur entrée dans la scolarité obligatoire dès le 1er cycle et, d'autre part, un grand nombre de foyer est équipé d'une connexion Internet et de divers appareils connectés. Selon les interviewés, cette immersion dans l'espace 2.0 n'est pas toujours accompagnée – particulièrement dans le cadre privé – d'explication, de recommandation et de supervision. Du fait de leur jeune âge, et parfois un manque de maturité, ils ne

sont pas conscients et ne reconnaissent pas les dangers qu'ils peuvent rencontrer sur Internet. Plusieurs experts interviewés tirent des parallèles avec le monde physique, relevant qu'il est habituel de recommander à un enfant de ne pas parler à un inconnu, ne pas accepter un cadeau venant d'un inconnu ou de ne pas traverser la route sans regarder. Ces conseils peuvent tout à fait être adaptés au monde virtuel, à savoir de ne pas parler à un inconnu ou du moins de se méfier qu'une personne peut en cacher une autre derrière un ordinateur.

> *« Avant c'était vraiment l'homme dans la voiture et l'homme dans la cour d'école. Maintenant c'est l'homme derrière le téléphone portable »* (Pol-1)
>
> *« Je pense que nous devons construire la sécurité sur le net de la même manière que pour la circulation routière »* (PrévSo-5)

Le second argument avancé par les experts interviewés est la situation extraordinaire engendrée par la **pandémie du Coronavirus** débutée en 2020. Les mesures de restrictions et de confinement ont contraint tant les adultes que les mineurs à **passer plus de temps à la maison et derrière un ordinateur** ou un smartphone. Les activités de loisirs ont cédé leurs places à la curiosité, voire parfois à l'ennui. En effet, selon deux de nos experts du milieu policier, des mineurs ont été confrontés à du matériel pornographique pour la première fois durant la pandémie.

Globalement, les experts interviewés constatent ou présument que les cyber-délits sexuels à l'encontre de mineurs sont en augmentation. Toutefois, cette tendance n'est pas toujours visible dans les statistiques, laissant penser que l'augmentation est à considérer dans le chiffre noir de la criminalité.

Néanmoins, plusieurs experts interviewés ont évoqué des tendances ou points d'attention relatifs aux quatre phénomènes à l'étude :

- *Production de matériels pédopornographiques* : les interviewés – suisses et européens – s'accordent sur le fait que depuis quelques années du nouveau matériel – provenant notamment des Etats-Unis – est en circulation, et ce principalement sur le Dark web. Par conséquent, cela signifie que la production est en augmentation. Un fait qui a également été constaté par Interpol. Les experts français interviewés relèvent aussi une augmentation de la production sur leur territoire. Un besoin de reconnaissance par les pairs et la popularisation du Dark web[245] peuvent expliquer une partie du phénomène. En revanche, sur le territoire helvétique, la production de pédopornographie au sens strict ne semble pas être détectée.
- *Distribution de matériels pédopornographiques* : la communauté pédocriminelle opère principalement sur le Dark web. Les méthodes d'échange et de distribution évoluent dans le sens où le *peer-to-peer* est gentiment abandonné. Mais la police n'a pas encore identifié formellement ces nouveaux vecteurs, ce qui impliquera potentiellement de déterminer de nouvelles stratégies d'investigation.
- *Cyber grooming* : les activités d'investigation policière indiquent que ce phénomène prend de l'ampleur tant en Suisse romande qu'en France. Pour la Suisse alémanique, les experts interviewés ne se sont pas clairement prononcés, mais présument une augmentation.
- *Sextorsion* : ce phénomène est souvent perçu comme comportant un aspect économique. Néanmoins, lorsqu'il s'agit de victimes mineures, la sextorsion sera plutôt employée pour

[245] Des experts français constatent une recrudescence des sites avec des parties francophones.

obtenir davantage de matériels pédopornographiques, du nouveau matériel, et du matériel de plus en plus grave.

- *Live-streaming* : ce phénomène est très récent et encore peu connu. Les interviewés suisses mentionnent ne pas encore être confrontés à ce phénomène. En revanche, il ressort que fedpol a tout de même traité un nombre plus élevé de demandes de coordination – de l'étranger vers la Suisse, et de la Suisse vers l'étranger – en matière de live-streaming, ce qui semble alors rejoindre la tendance internationale. En effet, une experte interviewée – active dans le milieu policier en France – parle d'une forte croissance des affaires de live-streaming.

4.4.1.1 Sur Internet, mais où ?

De manière générale, les plateformes attractives, pour les auteurs de cyber-délits sexuels envers les mineurs, sont justement les plateformes fréquentées par les jeunes. Et ces plateformes changent au gré de la mode et des avancées technologiques. Alors que des chats basiques étaient utilisés au départ, les technologies permettant de générer soi-même/échanger du contenu, d'utiliser une caméra, etc. ont fait leur arrivée. Ainsi, le fait de pouvoir communiquer en direct et envoyer du contenu sont des critères pertinents. Les plateformes faciles d'accès, sans obligation de publier beaucoup de photos ou d'enregistrer un profil sont également des éléments avantageux pour les délinquants.

> *« Cela signifie que plus c'est direct et simple, plus c'est attrayant pour les auteurs »*
> (Juris-1)

Les entretiens avec les experts ont permis d'identifier cinq catégories de plateformes.

La première, celle dont on entend le plus parler, sont les **réseaux sociaux**. Les plus souvent mentionnés sont Instagram, TikTok, Snapchat et Kik. Facebook compte aussi parmi ces plateformes bien que sa popularité semble diminuer au fil des années[246]. Même si cela ne réduit pas le risque à zéro, certaines de ces grandes plateformes, comme Instagram et Facebook, ont investi en adoptant des mesures de protection et modération (fonction de blocage, possibilité de dénoncer, veille de contenu). De ce fait, ces plateformes sont souvent le point d'accroche avec le mineur, pour ensuite se déplacer sur une plateforme de messagerie cryptée ou retenue comme moins risquée par le pédocriminel (voir ci-dessous).

Une deuxième catégorie de plateformes populaires sont les **jeux vidéo en ligne**. En effet, l'une des premières études européennes focalisées sur le cyber grooming – et réalisée en 2012 – avait mis en avant la plateforme X-Box comme étant un canal utilisé par des auteurs pour entrer en contact avec des enfants. Alors qu'elles sont moins sous les projecteurs lors des discours sur les cyber-délits sexuels, les experts interviewés rapportent une augmentation de victimisation de mineurs sur ces plateformes (par ex. Fortnite, Minecraft[247]). Tout comme les réseaux sociaux, les plateformes de jeux vidéo contiennent des espaces de chat et, permettent parfois le partage de contenu. Un expert interviewé, spécialisé dans les jeux vidéo sérieux, constate une méconnaissance du monde des jeux en ligne chez les adultes, pouvant potentiellement être due à un gap générationnel entre les parents et les enfants. Un autre interviewé soulève que certains jeux vidéo collectifs impliquent déjà d'une certaine

[246] Facebook, l'un des premiers réseaux sociaux en ligne, est peu à peu abandonné par les nouvelles générations qui ne souhaitent pas fréquenter la même plateforme que leurs parents.
[247] En 2016, un enfant de 12 ans, domicilié à Bâle, avait été kidnappé à son domicile. Le ravisseur était entré en contact avec ce petit garçon sur la plateforme Minecraft. La police avait pu identifier le ravisseur grâce à l'historique de discussion.

manière un processus de construction de confiance, facilitant ainsi les contacts entre joueurs. De plus, il semblerait que les plateformes de jeux vidéo soient moins monitorées que les réseaux sociaux, laissant ainsi plus de place pour les comportements illicites. En outre, selon un expert interviewé – enquêteur de police –, les auteurs pensent souvent à tort que les entreprises propriétaires des grandes plateformes de jeu ne collaborent pas avec la police. Ceci expliquerait que les auteurs qui entrent en contact avec des mineurs sur les plateformes de jeux ont moins tendance à passer ensuite sur une messagerie cryptée.

Une troisième catégorie relevée par trois experts interviewés se rapporte aux **sites réservés aux adultes**. Alors que les réseaux sociaux et les plateformes de jeux vidéo en ligne sont généralement, voir exclusivement, conçus pour les jeunes, d'autres sites sont réservés aux adultes (par exemple, des sites érotiques ou des messageries instantanées pour rencontrer des inconnus (ex. Omegle)). Néanmoins, les systèmes de contrôle d'âge n'étant pas souvent sophistiqués, une présence de jeunes mineurs est aussi observée sur ce type de plateforme.

Une fois la discussion bien entamée, les échanges se poursuivent souvent sur des **messageries instantanées** telles que Telegram, Signal, WhatsApp, Discord.

Enfin, les experts interviewés ont également mentionné l'accès accru au **Dark web**. Il y a quelques années encore, le Dark web était perçu comme un espace numérique fréquenté uniquement par des personnes possédant un certain niveau de compétences informatiques pour entreprendre une action illicite. Aujourd'hui, d'une part, quiconque peut y accéder et, d'autre part, tout n'est pas illégal. Outre la distribution de pédopornographie, le Dark web permet aux pédocriminels d'échanger sur leurs pratiques et les astuces pour ne pas se faire appréhender. A ce propos, quelques guides du « parfait pédocriminel » seraient en circulation. Il est a relevé que des forums de commerce et d'exploitation de mineurs se sont aussi installés sur le Dark web.

Le choix de la plateforme dépend de facteurs multiples dont le niveau de compétences techniques de l'auteur et de ses intérêts. Par exemple, selon deux experts policiers, les plateformes de jeux vidéo seront plutôt investies par des criminels ayant un certain niveau technique et cherchant à entrer en contact avec des garçons.

Finalement, mentionnons que si certaines plateformes restent populaires pendant une période relativement longue, les experts interviewés reconnaissent que cela peut aussi changer très vite. Une plateforme ouverte aujourd'hui sera peut-être fermée demain, et une nouvelle sera mise en ligne. Par ailleurs, des experts interviewés mettent en garde contre les nouvelles technologies ou plateformes, tels que les métavers – où de potentiels risques ont déjà été mis en évidence –, mais aussi les nouveaux objets connectés.

4.4.1.2 Les victimes, les auteurs : existe-t-il un profil type ?

Partagée par la plupart des experts interviewés, la première réponse est qu'il n'y a **pas de profil type au sens strict**. Les affaires de cyber-délits sexuels ont démontré que les victimes et les auteurs proviennent de toutes classes d'âge, de toutes classes sociales, etc. En outre, il est toujours délicat d'établir des profils types, car les informations peuvent être généralisées et mal interprétées.

Certains interviewés ont tout de même fait part de quelques éléments qu'ils ont remarqué dans leur pratique, en précisant qu'il n'est pas possible de dire dans quelles proportions ces caractéristiques ont été observées.

Tab. 13 – Caractéristiques relevées dans la pratique des interviewés

Auteurs	Victimes
• L'âge tend à diminuer. Des auteurs âgés de moins de 30 ans sont de plus en plus constatés. • Prétendent souvent être plus jeunes que leur âge réel. • Généralement des hommes. Lorsque des femmes sont impliquées, elles sont souvent sous l'influence d'un homme. • Pas toujours des inconnus. Il peut s'agir d'un parent ou d'un proche de la victime[248]. • Peuvent avoir été eux-mêmes abusés. • Des jeunes adultes, sans expérience sexuelle, recherchent une solution de facilité en se tournant vers des femmes beaucoup plus jeunes. • Prétendent parfois être quelqu'un d'autre : une personnalité publique, une célébrité, un influenceur. • Font preuve de moins en moins de limites. • Gagnent la confiance de la victime en faisant de fausses promesses[250]. • Les auteurs de sextorsion ne cherchent pas forcément le contact (collectionneurs d'images).	• Fille et garçon. • L'âge tend à diminuer. • En matière de live-streaming, un certain nombre de victimes se trouvent en Asie, notamment aux Philippines. • En recherche d'attention, d'affirmation, d'appartenance[249]. • Peu de confiance envers les parents. • Isolées ou marginalisées dans le monde physique (par ex. victime de harcèlement). • Jeunes de la communauté LGBTQIA+. • Ont parfois un intérêt financier[251].

4.4.2 Politiques de prévention et de soutien : état des lieux, challenges et lignes directrices

La prévention occupe un rôle essentiel pour lutter contre la cyberdélinquance en ligne à l'encontre des mineurs, mais encore faut-il savoir comment la faire. En effet, les discussions avec les experts interviewés ne se sont pas centrées sur la pertinence en soi de la prévention – point acquiescé par tous –, mais plutôt sur les personnes qui doivent porter cette prévention, sur les modalités de mise en œuvre et sur les challenges identifiés.

4.4.2.1 Public cible et organisateurs

Il est évident que la prévention doit avant tout s'adresser aux mineurs qui sont les principaux concernés. Mais selon les experts interviewés, à elle seule, cette prévention n'est pas suffisante.

[248] Notamment dans une situation de production de matériel pédopornographique ou de live-streaming, pour des raisons financières ou d'échanges avec d'autres pédocriminels.
[249] Les jeunes marginalisés, ne se sentant pas compris par leur entourage, peuvent être plus réceptifs à l'attention que l'auteur leur portera.
[250] Nouveau téléphone, code de jeu vidéo pour passer à un niveau supérieur, etc.
[251] Des mineurs vendent volontairement leur corps sur internet pour gagner de l'argent (Instagram, Snapchat, etc.) et entrent en contact avec des pédocriminels de leur propre initiative. Ainsi, on peut trouver des noms d'utilisateur comme « Quick money », « Do yo need money? » (Juris-1). Un expert met en avant un besoin social chez des jeunes de s'afficher avec des vêtements ou autres objets de marque. Ces jeunes ne se perçoivent dès lors pas comme une victime.

> *« Avoir des prises de conscience générale de la population aussi parce que, en faisant de la prévention, on va avoir des gens de plus en plus informés et du coup moins sujets à être victimes »* (Pol-5)

Ainsi, une prévention générale – renvoyant au concept de prévention primaire – destinée à toute **la population**, et diffusée à large échelle de manière durable a été mis en avant par des experts[252]. Pour ce faire, une campagne nationale de sensibilisation, comme par exemple la campagne sur les cyber escroqueries des polices suisses, est une manière de pouvoir véhiculer largement un message.

Ensuite, la prévention plus spécifique peut être envisagée pour des groupes de la population dits à risque (en d'autres termes la prévention secondaire), à savoir ici **les mineurs**. Les enfants ont accès aux outils numériques de plus en plus tôt, sans pour autant toujours savoir comment les utiliser, ce qui est permis ou non, et sans toujours être conscients des risques encourus. En parlant de grooming, une experte interviewée a relevé que parfois des mineurs ne sont pas conscients qu'ils soient ou qu'ils ont été victimes d'abus.

> *« Si l'on se concentre sur le grooming, il arrive que les enfants et les jeunes ne sachent pas qu'ils sont dans une relation abusive sur le moment, et qu'ils ne réalisent qu'après coup, en y réfléchissant, qu'ils sont impliqués dans une relation abusive. Nous avons donc pensé que nous pourrions trouver une incidence plus élevée si nous parlions à de jeunes adolescents adultes qui pouvaient réfléchir à leurs expériences et nous avons trouvé une incidence légèrement plus élevée »* (PrévSo-4)

Non seulement les mineurs doivent être au centre de cette prévention, mais aussi **les parents**, **les enseignants**, **et tout professionnel du milieu de la jeunesse**. Ces personnes doivent pouvoir aussi disposer d'une éducation numérique, de connaissances et d'outils suffisants, d'une part, pour renforcer les messages clés auprès des mineurs, et d'autre part, pour être en mesure d'intervenir si une situation spéciale devait survenir. C'est sur ce point que les experts sont largement revenus et relèvent des lacunes. Il ressort que des parents, et inévitablement des enseignants, peuvent se sentir submergés par les avancées numériques et ressentir un gap générationnel. Par ailleurs, ils perçoivent parfois davantage les risques de piratage que les dangers à caractère sexuel. Les experts mettent donc en avant la pertinence de formation ou d'atelier afin d'aiguiller les parents.

En ce qui concerne les enseignants, alors que la formation intégrera bientôt ces éléments dans le cursus des futurs enseignants, des formations continues pourraient être envisagées pour les enseignants d'ores et déjà en activité.

Jusqu'à présent, nous avons discuté de la prévention comme elle est souvent entendue, à savoir sous l'angle de la victimisation en voulant empêcher que des mineurs deviennent des victimes. Cependant, la prévention s'adresse également aux **(potentiels) auteurs** en vue d'empêcher le passage à l'acte ou la récidive (prévention secondaire ou tertiaire). En ce sens, plusieurs experts ont soulevé le manque de prévention à cet égard. Les autorités communiquent régulièrement sur les affaires de

[252] Une experte souligne que certaines parties de la Suisse, comme le Tessin, sont parfois oubliées dans les initiatives nationales (PrévSo-1).

pédopornographie pour informer de l'arrestation d'un pédophile[253], la fermeture d'un site Internet[254], etc. Cette démarche vise un effet dissuasif en montrant aux (potentiels) auteurs que la police et la justice sont présentes, en soi que la police occupe le terrain. Alors que les annonces aux médias intervenaient plutôt dans le cadre d'enquêtes d'une certaine envergure ou à portée internationale, les enquêtes à l'échelle locale sont maintenant aussi communiquées. Néanmoins, d'autres initiatives doivent être trouvées. Une experte ajoute que les messages préventifs quant au passage à l'acte doivent également s'adresser aux mineurs, car ceux-ci s'adonnent déjà à des activités illicites à connotation sexuelle, telles que le sexting (selon le contexte), la sextorsion (et le revenge porn), et procèdent aussi à du téléchargement de contenus pédopornographiques. Quant aux mesures d'aide et de soutien, là aussi des lacunes sont constatées par les experts vis-à-vis du suivi psychologique apporté aux personnes condamnées pour des délits sexuels. Sur la question de savoir quel type de suivi ou de traitement peuvent être envisagés, les experts n'ont pas de réponse. Des traitements sont déjà mis en place pour les délinquants sexuels, mais reste à savoir si ceux-ci correspondent aussi aux besoins des cyberdélinquants sexuels[255]. Pour ce faire, une meilleure compréhension des cyber pédocriminels, notamment des pédophiles, est requise pour mettre en place des mesures de prévention adéquates.

Sur le principe, les experts s'accordent aussi en disant que la prévention est une responsabilité de tous (autorités étatiques, parents/ famille, établissements scolaires et de loisirs, pairs, fournisseurs de services, etc.). Toutefois, un jeu de pingpong prend parfois forme entre les différents acteurs, chacun d'entre eux attribuant la responsabilité à l'autre. Quelques experts indiquent qu'un appui politique serait nécessaire pour faire avancer les choses. En Suisse, une **approche multipartite** est déjà appliquée avec une pluralité d'acteurs actifs dans ce domaine (*supra*, ch. 4.2). Cette diversité permet de répondre à des besoins et des attentes différentes auprès de la population. Par exemple, plusieurs experts ont mis en avant la réticence de certains mineurs victimes – voire de leurs parents – à s'adresser aux forces de l'ordre, le seuil d'inhibition étant plus bas envers les associations et plus encore envers le corps enseignant, et les pairs.

4.4.2.2 Mesures de prévention secondaire et tertiaire

Du fait que les mineurs commencent à utiliser les technologies numériques de plus en plus jeunes, la prévention devrait aussi intervenir plus tôt.

Les experts sont d'avis que la prévention doit prendre place **là où sont les mineurs** : à la maison, à l'école, dans les centres de loisirs, mais aussi sur les réseaux sociaux et les plateformes de jeux vidéo. Cela implique de connaître comment fonctionnent les mineurs, quels sont leurs habitudes et comment cherchent-ils les informations. Les experts s'accordent également sur le fait qu'il n'y a pas qu'une seule mesure à développer, mais plusieurs afin de toucher un maximum de personnes.

[253] Par exemple, en mars 2022, la police neuchâteloise a communiqué sur l'arrestation d'un homme pour avoir organisé une rencontre avec ce qu'il croyait être une mineure, alors qu'il s'agissait d'un enquêteur infiltré. https://www.ne.ch/autorites/DESC/PONE/medias/Pages/20220302_commpresse_interpellation-neuch%C3%A2tel-p%C3%A9docriminel-pr%C3%A9sum%C3%A9.aspx?msclkid=7bf5986eced211ec8a52ab958498c2b2

[254] La police a communiqué sur la fermeture de deux plateformes à contenus pédopornographiques hébergés en Suisse. https://www.tdg.ch/deux-plateformes-a-contenus-pedocriminels-fermes-en-suisse-844634825470

[255] Il ressort de travaux de recherche sur les cognitions et émotions problématiques chez les cyberdélinquants sexuels, que des traitements différenciés pour les cyberdélinquants et les délinquants hors ligne sont recommandés (Paquette, 2022).

> *« Je pense que c'est comme un puzzle qui s'emboîte. […] Je pense qu'il y a besoin de tout ce paquet de mesures, qui est tout simplement bien répété »* (Juris-1)

« Tout commence à la **maison** et continue à l'école » selon une experte que nous avons interviewée (PrévSo-2). La supervision parentale est ainsi primordiale, ce qui renforce le besoin de sensibiliser également les parents. Plusieurs experts ont parlé à de multiples reprises de la relation de confiance entre un mineur et ses parents, ainsi que de l'importance du dialogue. Un mineur doit pouvoir se confier à ses parents, même s'il est conscient d'avoir fait une erreur. Le dialogue a une place essentielle non seulement dans la prévention des dangers mais aussi pour préparer le mineur si un jour il devrait être confronté à une situation délicate.

> *« La vraie question, c'est qu'est-ce que vous devez faire pour préparer votre enfant lorsqu'il va avoir accès à ça ? Parce que les parents auront beau faire le maximum, ce sera dans la cour de récréation, avec les copains, les copines, ailleurs, toute façon qu'ils auront accès aux contenus. Donc ça passe par quelque chose qui est primordial, c'est le dialogue »* (Pol-7)

Quant au rôle des **écoles**, nous observons une implication des écoles, mais celles-ci restent la plupart du temps sur une prévention générale, sans introduire les dangers liés aux délits sexuels. Or, les experts soulignent le fait que les divers dangers d'Internet doivent être abordés très tôt. L'éducation numérique fait d'ailleurs son entrée de manière progressive en tant que discipline à part entière dans les programmes des écoles suisses[256,257]. Celle-ci s'appuie sur trois axes indépendants : l'usage des outils numériques, l'initiation à la science informatique et l'éducation aux nouveaux médias. Sur la base des informations disponibles, il n'est toutefois pas possible d'établir dans quelle mesure cet enseignement intégrera les dangers liés aux cyber-délits sexuels. Il ressort également des entretiens que les écoles privées ont une marge de manœuvre plus grande pour introduire des cours de prévention, le cursus étant déjà très chargé dans les écoles publiques. Par ailleurs, les écoles publiques semblent être également moins enclines aux interventions d'entreprises privées (notamment en Romandie) ou d'associations. Des raisons de coûts et d'image ont été évoquées. Enfin, dans le cadre d'intervention scolaire ou collective, il est important de conférer aux mineurs un rôle actif afin qu'ils se sentent concernés (par exemple, en partageant leurs idées, leurs ressentis).

Au-delà du foyer et de l'école, les experts s'accordent sur le fait que la prévention doit intégrer le quotidien et s'étendre aussi **aux activités extra-scolaires**.

Enfin, si les mineurs fréquentent assidument les **réseaux sociaux** et les **plateformes de jeux vidéo**, la prévention doit en faire autant. Ainsi, plusieurs experts soulignent que les initiatives de prévention doivent investir ces "nouvelles" plateformes. Par exemple, la campagne de lancement de l'avatar Enfant bleu sur Fortnite a fait preuve d'innovation en intégrant les plateformes de réseaux sociaux, ainsi qu'en collaborant avec des influenceurs du monde du jeu vidéo. Il en va de même pour les mesures d'aide. Dès lors que ces plateformes représentent un risque avéré, un système d'aide immédiate devrait être installée avec une présence 24/24h (un bouton help ou un avatar comme le

[256] Le programme scolaire en Suisse se base sur trois plans d'études distincts en fonction de la région linguistique: le Plan d'études romand (Suisse romande), le Lehrplan 21 (Suisse allemande), le Piano du studio (Suisse italienne).
[257] Avant de devenir une discipline à part entière, l'éducation numérique était dispensée dans le cadre d'autres matières.

projet pilote de l'Enfant bleu). Cette observation s'applique tout autant aux autorités de prévention (dont la police), d'assurer une permanence sur Internet.

4.4.2.3 La question de l'efficacité des mesures de prévention et de soutien

L'efficacité des mesures de prévention était la thématique la plus épineuse des entretiens. De manière générale, les experts n'ont pas pu se prononcer à ce sujet, car les évaluations scientifiques sur les programmes de prévention en la matière sont très pauvres. C'est un constat général que l'on peut faire sur les programmes de prévention, et encore plus en lien avec la cybercriminalité qui est un phénomène relativement récent.

Un avis partagé par plusieurs experts est qu'il n'y a pas réellement de mesures inefficaces. Si la mesure aide ne serait-ce qu'un enfant, alors c'est déjà une bonne chose. Un autre point mentionné est la répétition des messages de prévention. Plus les mesures sont réitérées, plus il y a de chances qu'elles atteignent leurs objectifs.

En revanche, certains experts ont tout de même mis en avant que la prévention plus traditionnelle et passive, telle que les brochures d'information ou les flyers vont moins éveiller l'intérêt des mineurs. Cette documentation se destine plutôt aux parents. Ainsi, les mesures de prévention doivent être actives et interactives. Les mineurs doivent se sentir intégrés dans le processus de prévention. Une experte, en parlant plus spécifiquement de la prévention auprès des adolescents, stipule que cela requiert un processus de « co-production et de collaboration ». En effet, la prévention auprès des plus grands se révèle plus difficile, et ce pour plusieurs raisons. En parlant de l'évaluation d'un programme, une experte a indiqué que même si les adolescents comprennent les risques, ils en feront qu'à leur tête.

> *« ils [les adolescents] ont vraiment compris tous les risques. Vous savez, ils savaient quels étaient les messages, mais ils n'ont pas agi en conséquence parce que devinez quoi ? Ce sont des adolescents, et les adolescentes font ce qu'ils veulent. »* (PrévSo-4)

La participation active des enfants est par ailleurs l'un des trois piliers de la nouvelle stratégie européenne pour un meilleur Internet pour les enfants (BIK+). Dans cette perspective, elle souhaite, d'une part, encourager la prévention par les pairs et, d'autre part, évaluer la stratégie tous les deux ans avec le concours des enfants[258].

Un autre enjeu de la protection des adolescents est que les mesures techniques ne fonctionnent plus aussi bien qu'avec les enfants plus jeunes. Les adolescents acquièrent des compétences techniques qui leur permettent de contourner facilement certains filtres de contrôle parental (dès l'âge de 12-13 ans).

Alors que la prévention a déjà bien investi le milieu scolaire – du moins en termes d'éducation numérique – les experts sont d'avis que pour que les mesures de prévention soient efficaces elles doivent utiliser les mêmes canaux de communication que les jeunes.

Enfin, plusieurs experts ont relevé que les messages préventifs auprès des jeunes devraient davantage souligner que la diffusion de vidéos et d'images sur Internet peut avoir des conséquences à long terme. En ce sens, les experts faisaient principalement référence au fait qu'il n'est pas possible d'effacer

[258] https://ec.europa.eu/commission/presscorner/detail/fr/IP_22_2825

complètement une image. Dès qu'une image ou une vidéo est publiée sur Internet, elle reste pour toujours dans l'espace numérique.

4.4.2.4 Les challenges du développement et de l'implémentation des mesures

Les experts ont souligné plusieurs éléments à prendre en considération dans l'élaboration d'une mesure d'intervention.

Les experts soulignent un **manque de collaboration et de coopération** ayant pour conséquence des initiatives multiples et appliquées en silos. Cette collaboration lacunaire se manifeste non seulement entre les intervenants de secteurs d'activité distincts, mais également entre les intervenants d'un même domaine. A ce sujet, les experts font part d'une certaine compétition entre les associations actives dans la protection des mineurs, entravant ainsi l'échange d'information, de bonnes pratiques et la mutualisation des ressources.

Cet enclavement des initiatives se répercutent également sur les messages qui sont véhiculés aux mineurs. Le discours d'un intervenant n'est pas forcément le même que celui d'un autre. Ainsi, plusieurs experts relayent un besoin d'uniformiser les messages de prévention à l'échelle nationale, voire internationale. De plus, les messages doivent être d'actualité. Un expert a pris l'exemple de la méthode du psychiatre Serge Tisseron sur l'utilisation des écrans. Alors que la méthode a été révisée, des affiches de la méthode initiale serait encore accrochée dans certaines écoles.

La multiplication des initiatives apporte aussi une certaine confusion lorsqu'il est question de chercher une information ou de l'aide. Plusieurs experts suisses mentionnent qu'il n'est pas facile de savoir à quelle institution, quel service ou quelle autorité s'adresser.

4.4.3 Politiques de répression : état des lieux, challenges et améliorations attendues

Dans cette section, nous nous intéressons aux mesures relevant davantage du milieu de la police et de la justice. En effet, les experts interviewés sont revenus sur plusieurs aspects du cadre légal et de la procédure pénale. Les collaborations avec d'autres partenaires, tels que les fournisseurs de services de télécommunication ont été abordées. Enfin, nous terminons avec quelques considérations sur le volet des nouvelles techniques de détection.

4.4.3.1 Cadre légal, les révisions attendues ou suggérées

Le premier constat ressortant des entretiens est que le droit suisse en vigueur traite globalement les cyber-délits sexuels de manière satisfaisante. Plusieurs législations ont été révisées suite à la ratification des instruments internationaux tels que la Convention de Budapest et la Convention de Lanzarote. Toutefois, certains aspects législatifs sont encore perfectibles selon les experts interviewés. Nous exposons ici les principaux points concernant les dispositions législatives[259].

[259] Un autre point avancé par une experte concernait l'utilité d'introduire une norme d'exemption pour les policiers travaillant dans le domaine de la pornographie enfantine, une disposition légale semblable existant déjà pour les agents infiltrés dans le cadre d'investigations en matière de stupéfiants (art. 294 CPP). Selon cet expert, une telle exemption de punissabilité faciliterait les investigations et éviterait que les enquêteurs se questionnent régulièrement sur la possibilité d'envoyer d'une image et sur les répercussions encourues. Dans le cadre de la révision du Code de procédure pénale en cours, une reformulation du libellé de l'art. 294 CPP est proposée afin d'étendre la disposition aux agents infiltrés agissant « dans le cadre d'une investigation secrète autorisée lors de la poursuite de pornographie impliquant des mineurs ou d'actes d'ordre sexuel avec des mineurs : conformément à l'art. 197, al. 4 et 5, CP, pour autant que les objets ou les représentations n'aient

Alors que la règlementation en matière de production et distribution de pédopornographie, de sextorsion et de live-streaming semble faire l'objet d'un consens général, les avis sont plus partagés en ce qui concerne le cyber grooming. Comme exposé dans le contexte juridique (*supra*, ch. 2.2), au moment de la réalisation de cette étude (juin 2022), un débat a pris place dans le cadre de la révision du droit pénal de savoir si une **disposition spécifique au cyber grooming** au sens strict doit être introduite. Plusieurs experts suisses interviewés ont soulevé l'importance de pouvoir bénéficier d'une base légale spécifique à ce comportement et comportant un champ d'application plus large. En effet, nous avons vu que plusieurs infractions du code pénal peuvent trouver application dans une situation de cyber grooming. En ce sens, une tentative d'actes d'ordre sexuel avec un enfant de moins de 16 ans peut être retenue pour criminaliser une situation de cyber grooming. Toutefois, cela signifie que l'auteur doit être sur le point de matérialiser l'infraction. En d'autres termes, cela implique que l'auteur se soit présenté au lieu de rendez-vous ou qu'il en soit très proche. De plus, comme mentionné en amont (*supra*, ch. 2.2.2), certains actes propices pour le pédopiégeage en ligne peuvent être réprimés, avant même de se rendre à un rendez-vous à des fins sexuelles avec un mineur. Cependant, les partisans à l'élargissement de la définition du cyber grooming proposent que d'autres actes antérieurs à la rencontre soient punissables[260], comme par exemple les échanges à caractère sexuel sur un forum de discussion, ainsi que le processus de mise en confiance et d'isolation de l'enfant mis en œuvre par les auteurs de cyber grooming pour arriver à leurs fins[261]. Selon deux experts juridiques interviewés, ce n'est pas tant le champ d'application de l'infraction mais plutôt la conception du développement harmonieux sexuel de l'enfant (bien juridiquement protégé dans le cas d'espèce) qui devrait être revu. En d'autres termes, qu'est-ce qui met en danger ce développement ? L'acte matériel ou déjà les propositions indécentes et le processus de mise en confiance, voire de manipulation de l'enfant ? Les experts proposent donc la création d'une nouvelle norme visant à criminaliser spécifiquement ces comportements, en complément des infractions plus graves déjà en vigueur. Une telle disposition permettrait aussi de viser les auteurs qui se satisfont, et éprouvent un plaisir sexuel à échanger des propos à caractère sexuel avec des enfants, sans aller plus loin.

Un autre élément mis en avant par l'un des experts est l'absence de **base légale autorisant, sous certaines conditions, des institutions à recevoir du matériel pédopornographique** et effectuer un triage. Cet aspect s'inscrit principalement dans la perspective d'une plateforme de signalement. A l'heure actuelle, plusieurs plateformes existent en Suisse mais ne sont habilitées à recevoir uniquement des liens URL, qu'elles doivent ensuite transmettre aux autorités compétentes. Dans cette perspective, autoriser la réception et le triage de matériel pédopornographique par une entité non-policière permettrait de décharger la police en leur transmettant uniquement les contenus illicites. Une entreprise privée ou une fondation (comme NCMEC aux Etats-Unis, le Centre canadien de protection de l'enfance au Canada ou l'Internet Watch Foundation au Royaume-Uni[262]) pourrait avoir la charge du triage du matériel reporté. Selon cet expert, cette lacune juridique empêche également la Suisse

pas pour contenu des actes d'ordre sexuel effectifs avec des mineurs ». Au moment de rédiger ce rapport (juin 2022), la modification a déjà été acceptée par le Conseil National et le Conseil des Etats.

[260] La question se pose également d'un point de vue répressif, en d'autres termes savoir si une base légale plus large permettrait de procéder à l'arrestation de plus d'auteurs. Dans des pays comme la France qui criminalise la simple demande à caractère sexuelle, les enquêteurs arrivent à déterminer l'identité de l'auteur de façon indirecte grâce à un travail d'environnement et un recoupement de données (horaire de travail, profil réseaux sociaux, etc.).

[261] Commission des affaires juridiques du Conseil des États (2022); Meyer (2020).

[262] Par exemple, au Royaume-Uni, un Mémorandum d'entente a été établi entre Internet Watch Foundation, le Crown Prosecution Service et le National Police Chief's Council.

d'intégrer des réseaux internationaux de lutte contre l'exploitation sexuelle des mineurs en ligne, comme par exemple le réseau mondial INHOPE[263]. Selon les habilitations, ces structures permettent de procéder à un premier triage du matériel recensé en vue de transmettre uniquement les contenus illicites aux autorités compétentes et ainsi décharger ces dernières.

Finalement, la majorité des experts pointe du doigt le manque de **réglementation entourant Internet**, notamment envers les fournisseurs de services de télécommunication et l'industrie des plateformes.

> *« Et aussi, c'est le seul média [Internet] qui a été donné au public, sans mettre de loi, sans mettre de règle à disposition. Quand la télé et la radio sont arrivées, il y avait des règles avant qu'on l'utilise »* (PrévSo-1)

D'une part, les experts souhaiteraient un renforcement de la réglementation envers les fournisseurs de services, en les obligeant à dénoncer tout contenu illicite. En Suisse, les fournisseurs de services sont déjà contraints par une telle réglementation (*supra*, 4.2.1). L'enjeu principal ici réside dans le caractère transnational de la cybercriminalité. En effet, les autorités doivent conjuguer avec la réglementation propre à chaque pays. Le deuxième Protocole additionnel à la Convention sur la cybercriminalité[264] prévoit une base juridique notamment « pour la coopération directe avec les fournisseurs de services pour les informations sur les abonnés »[265] et pourrait répondre en partie à ces enjeux. Le second aspect soulevé par les experts concerne les mesures de sécurité implémentées sur les plateformes afin de protéger les mineurs. Dans le sens où les entreprises devraient considérer la sécurité des mineurs dès la conception d'une plateforme ou d'une application. Un exemple couramment cité par les experts est le système de vérification d'âge. A nouveau, l'un des experts fait un parallèle avec le monde hors ligne.

> *« Si vous pensez au monde hors ligne, lorsque vous achetez de l'alcool, des cigarettes, des choses comme ça, nous avons un système d'identification créé par le gouvernement qui est utilisé et il y a des sanctions en place si vous ne suivez pas ce système en tant qu'entreprise. C'est vrai. Si vous faites le parallèle avec Internet, vous n'avez pas de mécanisme de vérification de l'âge et aucun problème si vous vous trompez »* (PrévSit-1)

Un dernier aspect, relevé principalement par les experts policiers et juridiques, se rapporte aux règles de conservation des données, à savoir quelles données et pendant combien de temps sont-elles sauvegardées. Là aussi, les règles peuvent changer d'un pays à l'autre. En ce sens, un effort d'harmonisation permettrait de faciliter certaines investigations et procédures pénales.

4.4.3.2 Les challenges des investigations et procédures pénales

Dans la lutte contre les cyber-délits sexuels, le droit en vigueur apporte un premier arsenal de mesures en criminalisant des comportements déterminés. Mais ensuite, comme le relève un expert, il faut distinguer la norme théorique de son application.

[263] Le réseau INHOPE est composé de 50 hotlines réparties dans 46 pays à travers le monde (www.inhope.org).
[264] Deuxième Protocole additionnel à la Convention sur la cybercriminalité – relatif au renforcement de la coopération et de la divulgation de preuves électroniques, STCE n°224. Le traité a été ouvert pour signature le 12 mai 2022. Au moment de rédiger ce rapport (juin 2022), la Suisse n'avait pas signé ce deuxième protocole additionnel.
[265] https://www.coe.int/fr/web/conventions/full-list?module=treaty-detail&treatynum=224

> *« Je crois qu'il faut distinguer la norme qui peut être appliquée et qui couvre à peu près tous les cas de figure. Et puis, le fait de est-ce qu'on est capable d'identifier et de poursuivre »* (Juris-2)

Les entretiens avec les experts ont permis de mettre en relief six enjeux et challenges dont souffrent les investigations et les procédures pénales.

Le premier challenge mentionné par plusieurs experts est **la connaissance des faits**. Il ressort que les mineurs sont plutôt réservés lorsqu'ils se retrouvent dans une situation similaire. En effet, les jeunes confient rarement ce type de problèmes aux parents ou à d'autres personnes de confiance. Les experts ont formulé deux hypothèses explicatives : (1) le mineur ne se considère pas en tant que victime, ne s'en rend pas compte, (2) le mineur éprouve un sentiment de honte et de culpabilité, pouvant le pousser parfois à une issue fatale. Les experts ont rapporté également des situations où le mineur se confie aux parents, qui eux décident de ne pas dénoncer la situation. Ici, les parents peuvent éprouver un sentiment d'échec ou alors veulent préserver le mineur du poids et des répercussions d'une procédure pénale. Etant donné qu'une plainte pénale est rarement déposée, d'autres stratégies doivent être adoptées pour détecter les délits sexuels commis en ligne à l'encontre des enfants.

Comme exposé plus haut, la police possède plusieurs outils ou méthodes de travail permettant de détecter des cyber-délits sexuels (*supra*, ch. 4.3.2.3). Les experts, tant de la Suisse que de l'étranger, soulignent un **manque de ressources humaines pour gérer la quantité d'affaires** qui se présentent à eux. En effet, l'essor d'Internet a généré une demande de ressources plus importantes dans le secteur cyber. Comme dans d'autres domaines policiers, cela se traduit par le développement de modèles de prises de décisions pour aider les enquêteurs à prioriser leurs activités. Par exemple, en Suisse, en se basant sur une échelle de sept niveaux, les enquêteurs infiltrés essayent de distinguer les fantasmeurs des potentiels prédateurs sexuels. Dans une même logique, un autre exemple – tiré de la pratique en France pour les contenus pédopornographiques – est de distinguer les hauts profils des bas profils. La découverte de contenu inédit sera considérée comme un haut profil, dès lors qu'il y a un soupçon de production.

Une fois que les autorités prennent connaissance d'un cyber-délit – sexuel ou non – une question primordiale se pose, celle de la **juridiction**. En effet, le principe de territorialité confère à un Etat la compétence principale de poursuivre toute infraction commise sur son territoire (art. 3 CP), qui est défini par les frontières et des règles précises. De plus, la compétence en la matière étant conféré aux cantons, il s'agit également de déterminer quel est le canton compétent. Mais en matière de cybercriminalité, ces frontières terrestres n'existent plus, impliquant fréquemment une composante extraterritoriale : que ce soit que l'auteur ou la victime se trouve à l'étranger, ou encore que les données pertinentes à l'enquête (par exemple des images pédopornographiques) soient stockées sur un serveur hébergé à l'étranger. Plusieurs experts nous ont confié que la question de la juridiction n'est pas toujours limpide au début d'une affaire.

> *« Et bien sûr, il faut aussi beaucoup de motivation pour investir ces ressources s'il n'est pas clair au départ que l'infraction relève de sa propre juridiction »* (Juris-1)

Lorsque les autorités se saisissent d'une affaire, il est déterminant de pouvoir identifier l'auteur (ou les auteurs). L'**identification de l'auteur** peut être très rapide, comme très longue. En effet, les auteurs

ont de plus en plus recours à des mesures d'offuscation en passant par exemple par des réseaux VPN, des Proxys ou TOR. En outre, des manuels et des tutoriels sont disponibles sur le Dark Web avec des astuces pour éviter de se faire démasquer ou pour confondre les pistes (par exemple, comment faire croire qu'une photo a été prise dans un autre pays). Ce sont de nouvelles techniques que les enquêteurs doivent prendre en considération et trouver des moyens pour les surmonter. Relevons tout de même qu'en Suisse, des procédures pénales peuvent être instruites contre X, même si cela ne permettra pas d'arrêter et de condamner l'auteur.

Le cinquième point discuté avec les experts est la **difficulté d'obtenir des preuves**. Elle peut se manifester sous deux formes. D'une part, les preuves existent mais l'accès est compliqué. Cette perspective renvoie notamment à la coopération internationale et la collaboration avec les services de télécommunication. Au vu de l'importance de ces deux sujets dans les entretiens, nous avons préféré les approfondir dans des sections séparées (*infra*, ch. 4.4.3.3 et 4.4.3.4). D'autre part, certains comportements commis en ligne en direct, comme pour le live-streaming, ne laissent pas toujours de preuve directe. A moins que l'auteur enregistre la performance ou qu'il soit pris en flagrant délit (lors d'une perquisition ou d'une mesure de surveillance, par exemple), il sera plus complexe de créer un faisceau d'indice suffisant.

Le dernier challenge se réfère à la poursuite pénale et plus précisément aux **évaluations psychologiques des prévenus**. Il est nécessaire de comprendre leurs comportements et de déterminer s'ils souffrent de troubles particuliers (pédophilie, désordre sadique, etc.), mais ces évaluations prennent du temps et coûtent cher.

4.4.3.3 La collaboration avec les fournisseurs de services de télécommunication

Dès lors que les cyber-délits – sexuels ou non – sont réalisés au moyen d'appareils numériques, il est fréquent de faire appel à un fournisseur de services de télécommunication pour obtenir des données. De manière générale, les experts s'accordent sur le fait que la collaboration avec les fournisseurs suisses fonctionne très bien. Par ailleurs, les fournisseurs en Suisse ont l'obligation d'informer les autorités compétentes s'ils découvrent du contenu illicite sur leur serveur.

Au niveau international, il ressort que la **Convention de Budapest** a facilité l'accès aux informations. En effet, l'art. 32b[266] permet aux fournisseurs de services de transmettre les données à un autre pays. Toutefois, il ne s'agit pas d'une obligation, et le fournisseur peut refuser la demande. C'est pourquoi, l'opinion des experts est plus nuancée en ce qui concerne la collaboration avec des fournisseurs de services basés à l'étranger. Certains fournisseurs sont très ouverts à collaborer, notamment ceux qui se trouvent aux Etats-Unis. La Suisse peut faire directement une demande auprès de certains fournisseurs de services. Il est à préciser que ce canal prévaut uniquement pour les informations basiques. En matière de demande de contenu ou de surveillance, une demande d'entraide judiciaire est requise. Certains fournisseurs transmettent aussi parfois des informations de manière spontanée, surtout dans ce domaine où le caractère nuisible et illicite fait l'objet d'un consensus. Un autre point

[266] « Une Partie peut, sans l'autorisation d'une autre Partie (a) accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou (b) accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique ».

positif de la collaboration est l'établissement chez certains fournisseurs de services d'un point de contact unique.

En revanche, les relations peuvent s'avérer plus laborieuses avec d'autres fournisseurs de services réticents à collaborer. Certains experts ont relevé notamment des difficultés avec les fournisseurs de services dont le siège social se trouve dans un pays n'ayant pas ratifié la Convention de Budapest. Un exemple mentionné par plusieurs experts est l'Irlande, qui compte sur son territoire le siège principal de quelques fournisseurs très populaires. Dans le cas d'un refus de collaboration ou lorsque le fournisseur a son siège dans un pays ne faisant pas partie de la Convention de Budapest, une **demande d'entraide judiciaire** doit être initiée. Le temps que l'autorité compétente examine la demande et oblige le fournisseur à transmettre les données, un laps de temps de plusieurs mois, voire plusieurs années peut s'écouler. Cette longue attente peut dès lors porter préjudice à l'investigation en cours. Par ailleurs, l'un des experts rapporte un jeu de pingpong qui peut parfois s'installer entre les différents sièges d'une entreprise, faisant ainsi perdre davantage de temps.

> *« Il s'agit donc de ces débats constants, qui ne nous facilitent pas la vie, mais qui, au contraire, facilitent le travail des auteurs de ces crimes »* (Juris-1)

Enfin, mentionnons que la **collaboration avec l'organisation NCMEC** permet de faire le pont de manière indirecte avec les fournisseurs de services américains. Comme mentionné dans le contexte en début de rapport (*supra*, ch. 2.3.2), fedpol reçoit de manière systématique des annonces de contenus suspects de la part de NCMEC. Cette organisation collecte directement ces informations auprès des fournisseurs de services américains, car ils ont l'obligation de dénoncer tout matériel illicite figurant sur leur serveur.

Pour conclure cette partie, le concours des fournisseurs de services est essentiel dans la détection des cyber-délits sexuels, car ils détiennent des informations et peuvent intervenir en tant que partie prenante ayant un rôle plus neutre que le mineur ou les parents. Un travail de renforcement de la collaboration internationale ne peut être que bénéfique, et permettra de montrer qu'il n'y a pas d'espace sans loi.

4.4.3.4 La coopération policière

La coopération policière peut intervenir à l'échelle intercantonale, nationale et internationale. Chacun de ces niveaux a été discuté avec les experts interviewés.

Au niveau international, il convient de distinguer la coopération bilatérale de la coopération multinationale. Comme pour le sujet précédent, la Convention de Budapest a facilité également la collaboration entre Etats et l'accès aux informations. Les experts interviewés sont d'avis que la coopération bilatérale – qui peut être activée à travers Interpol, Europol, Eurojust ou un canal police déterminé – fonctionne plutôt bien. Plusieurs experts interviewés ont souligné la bonne collaboration entretenue avec les autorités des Etats-Unis.

En matière de coopération multilatérale, des groupes de travail sont créés afin de rassembler des spécialistes de police sur des thématiques. En matière de pédopornographie, des cellules spéciales en identification de victimes travaillent plusieurs jours sur du nouveau matériel afin d'essayer d'identifier un élément pertinent et contribuent à faire avancer des enquêtes. Les retours des experts interviewés

sont très positifs à ce sujet. La présence d'un agent suisse au centre d'Interpol de Singapour permet également de renforcer la collaboration. Un autre point essentiel de la coopération multinationale est la base de données d'images et de vidéos ICSE (Internet Child Sexual Exploitation) d'Interpol qui permet de déterminer si un matériel illicite est déjà connu ou pas. Enfin, Europol organise également des formations pour les enquêtes en matière de pédocriminalité.

La coopération internationale est essentielle pour lutter contre un phénomène transfrontalier tels que la cyberdélinquance sexuelle. L'échange d'information permet de faire avancer des investigations, mais aussi de se tenir au courant des nouvelles tendances, des nouvelles plateformes, des nouveaux modus operandi. Surtout quand ces informations proviennent de pays proches, elles permettent de se préparer à de potentielles futures infractions en Suisse. Pouvoir bénéficier des expériences permet également de se professionnaliser et d'économiser des ressources.

> *« Moi, je suis un fan absolu d'aller voir ailleurs comment ils font, plutôt que de recréer toujours la même chose. […] Et puis de plus, on va se mettre ensemble, plus on va profiter de l'expérience des uns et des autres, plus on va économiser des ressources et se professionnaliser »* (Pol-5)

À l'échelle helvétique, la collaboration s'est énormément développée ces dernières années grâce au réseau NEDIK. Les rencontres mensuelles du réseau favorisent les échanges entre les cantons. La récente création du bataillon cyber de l'Armée suisse permettra peut-être aussi d'intensifier les échanges au niveau national, tout comme la future transformation du NCSC en office fédéral[267].

Des progrès sont également à mentionner au niveau de la Romandie avec la création du Centre régional de compétence cyber (RC3) créé en 2021. Ce centre, qui est encore récent et en développement, permet de mutualiser les infrastructures et les ressources en matière de cybercriminalité. En revanche, l'un des experts interviewés relève une faiblesse au niveau du partage de données entre les cantons. De manière générale, « les policiers n'ont accès qu'aux bases de données exploitées par leur propre canton »[268]. Toutefois, le concordat RBT permet aux corps de police qui en sont membres d'échanger des données, l'équivalent n'étant pas observé du côté alémanique. En effet, plusieurs concordats sont présents, et certains cantons ne font partie d'aucun concordat. Par conséquent, ces cantons ne bénéficient pas des mêmes bases légales que la Romandie (y compris le Tessin et Berne) pour travailler ensemble. Toutefois, il est à relever que deux projets permettant un partage d'informations à l'échelle nationale sont en cours de développement. Le premier est l'extension du projet PICSEL – plateforme d'informations de la criminalité sérielle en ligne – à toutes les polices suisses, le deuxième est le projet Plateforme d'interrogation de la police (POLAP) qui permettra aux polices suisses d' « accéder directement aux données de police sur les personnes, véhicules, biens et leurs opérations ainsi qu'aux données de migration de la Confédération et des systèmes de l'OFROU »[269]. Cette plateforme permettra « aux organisations d'utilisateurs concernées de consulter par une seule demande les informations en ligne disponibles dans les systèmes informatiques cantonaux, nationaux et internationaux »[270].

[267] Conseil fédéral et Secrétariat général DFF (2022).
[268] Commission de la politique de sécurité du Conseil des États (2019, p. 3).
[269] Röösli (2022, p. 5).
[270] Röösli (2022, p. 5).

Même si des progrès manifestes peuvent être relevés, les experts interviewés sont d'avis qu'il est essentiel de poursuivre ces efforts de renforcement et d'intensification de la coopération nationale et internationale.

> *« Ce que je trouve personnellement très important, c'est que ce renforcement et cette expansion de la coopération internationale soient poussés en avant, tout simplement parce que cela nous ferait gagner beaucoup de temps et que le temps est crucial pour résoudre les affaires. »* (Juris-1)

4.4.3.5 Les techniques de détection

Les mesures de détection de comportements ou de contenus illégaux en matière de pédocriminalité ont été abordées sous deux angles dans le cadre des entretiens : d'une part, les moyens ou les outils à disposition de la police et, d'autre part, les logiciels ayant recours à l'intelligence artificielle.

Dans le domaine de la police, les experts interviewés ont ouvertement notifié que les techniques d'enquête, et certains outils à leur disposition, sont de nature confidentielle et ne peuvent être divulgués afin de ne pas faciliter les activités des pédocriminels. La discussion avec les experts interviewés s'est donc portée sur les techniques déjà connues du grand public, sans toutefois entrer dans les détails opérationnels.

Les mesures relevées correspondent aux méthodes suisses que nous avions déjà exposées au ch. 4.3.2.3, à savoir le monitoring (ou de la veille), les infiltrations, le suivi des signalements, et le blocage de site Internet. Nous apportons ici quelques observations faites par les experts interviewés.

Le **monitoring ou la surveillance systématique** et complète d'Internet n'est pas autorisée en Europe. En effet, une pesée des intérêts entre la protection de la vie privée et la protection des mineurs fait débat. En revanche, des méthodes de surveillance systématique sont plus courantes en Amérique du Nord. Dans l'Union européenne et en Suisse, des veilles plus spécifiques peuvent être réalisées. En Suisse, par exemple, un logiciel permet de traquer les téléchargements illicites. La procédure de veille peut également être enclenchée suite à la découverte d'images pédopornographiques.

Concernant les **infiltrations ou recherches secrètes**, elles se font généralement sur les sites de chat, où un enquêteur va se faire passer pour un mineur. Les enquêteurs doivent être formés et habilités pour mener ces recherches secrètes. Cette procédure demande un grand investissement en temps de la part des enquêteurs. De plus, le pédocriminel va parfois vouloir s'assurer qu'il discute bien avec un enfant et/ou demander des garanties. Pour ces dernières, il s'agit souvent de l'envoi de photo à caractère sexuel. Cette demande pose dès lors problème puisque, d'une part, il faut pouvoir disposer de ce matériel et, d'autre part, il s'agit d'un acte pénalement répréhensible. En Suisse, les enquêteurs vont alors envoyer des photos truquées. La photo d'un mineur peut être construite soit en assemblant des photos de membres de diverses personnes, soit en générant une photo à l'aide d'un logiciel. Cependant, cette deuxième solution comporte le désavantage que le logiciel va générer une nouvelle silhouette à chaque photo. Or, pour contrer cela, les pédocriminels demandent souvent des séries de photo. À ce sujet, la France est l'un des rares pays dont la législation permette aux enquêteurs d'utiliser de vraies photos tirées de la base de données nationales. Avant l'envoi, les photos sont anonymisées de manière à ce que le mineur ne soit pas identifiable.

D'autre part, la police reçoit un grand nombre de signalement, impliquant ainsi un travail de triage et de **suivi des signalements**. Plusieurs canaux d'information peuvent fournir ces signalements : les victimes en portant plainte ou en notifiant la police, les forces de police étrangères ou des organisations gérant des plateformes de dénonciation. Plusieurs experts interviewés ont souligné la plus-value de la collaboration avec l'organisation NCMEC, qui permet notamment de faire remonter des informations collectées auprès des fournisseurs de services américains. La collaboration avec le réseau INHOPE – composé de 50 hotlines à travers le monde – a également été mentionné par les experts français interviewés.

Enfin, les corps de police peuvent également procéder à un **blocage de site Internet** contenant du matériel pédopornographique, et avertissent ensuite le fournisseur de services de télécommunication ou de communication dérivée.

Le second volet porte sur les outils de détection développés à l'attention des forces de l'ordre mais également des fournisseurs de services ou tout autre entreprise intéressée. De manière générale, les experts interviewés ont connaissance de l'existence de ce type d'outils, mais pas suffisamment pour se prononcer sur les objectifs poursuivis, le fonctionnement ou l'efficacité de ceux-ci. Les experts interviewés mentionnent que le développement de tels outils est en pleine expansion rendant ainsi difficile d'avoir une vue d'ensemble sur l'offre exacte, et par conséquence de savoir quelles sont les techniques intéressantes pour la police. Hormis la difficulté de prendre connaissance de la multitude de projets, certains n'aboutissent jamais ou sont tenus secrets jusqu'à la commercialisation du produit. Enfin, d'autres projets développés pour le domaine policier sont parfois présentés lors de rencontres d'Interpol ou d'Europol, mais à nouveau, un haut degré de confidentialité est maintenu.

Par rapport aux techniques, il ressort que la reconnaissance faciale ou la détection de nudité (à l'aide de valeur hash) sont les principales techniques développées pour la détection d'images. Or, les avancées technologiques et l'introduction du partage de vidéo ont permis de tester de nouvelles techniques de détection basées sur des attributs qui ne sont pas présents dans des images statiques. Ainsi, certains projets se concentrent par exemple sur la reconnaissance vocale pour déterminer s'il s'agit d'une victime mineure ou pour établir des liens entre plusieurs vidéos. Une deuxième perspective est le développement des techniques de synthèse multimédia (deep fake) pour la création de contenu (par exemple pour les infiltrations policières). Enfin, une autre méthode se fonde sur l'analyse de texte afin de repérer des comportements spécifiques pouvant suggérer qu'un adulte discute avec un mineur avec de mauvaises intentions (détection du grooming).

Au-delà des perspectives prometteuses de ces nouvelles techniques, les experts interviewés ont relevé plusieurs points de réticence quant à leur utilisation. Tout d'abord, la réglementation ou l'accréditation pour l'utilisation de certaines techniques demeure incertaine. Le coût financier de ces outils peut aussi être un frein à leur utilisation, notamment pour les petites entreprises de télécommunication. Enfin, bien qu'une partie du travail soit effectuée automatiquement par des algorithmes, des ressources humaines sont toujours nécessaires pour effectuer des contrôles (notamment extraire les faux positifs) et traiter ensuite les éléments litigieux identifiés par l'algorithme.

4.4.4 Perspectives futures : défis et innovations

Les résultats présentés dans les sections précédentes ont permis de mettre en lumière plusieurs dimensions de la lutte contre la cyberdélinquance sexuelle et de la protection des mineurs. À présent, nous revenons sur les principaux défis relayés par les experts interviewés et apportons des pistes de réflexion pour le futur.

Le premier défi d'importance est la **rapidité des avancées technologiques et des modes opératoires** des cyberdélinquants. En effet, les développements techniques se font tous les jours, mais il faut du temps aux autorités pour détecter, comprendre et saisir un nouveau phénomène. Comme le relève un enquêteur français, « lorsqu'on parle de nouvelles technologies, de manière générale, c'est une course à l'innovation » (Pol-7).

Les experts interviewés ont mis en avant l'existence de tensions avec certains fournisseurs de services de télécommunication. C'est pourquoi la création, ou le renforcement, de **partenariats public-privé** pourrait être investi en vue de trouver un terrain d'entente au lieu de passer par la voie de l'entraide juridique. D'autre part, de tels partenariats permettraient d'obtenir des données complémentaires sur les phénomènes investigués, étant donné que les entreprises privées monitorent parfois d'autres données qui peuvent être intéressantes pour les autorités policières et judiciaires.

La protection des mineurs face aux cyber-délits sexuels est devenue une priorité dans plusieurs pays. Une pluralité d'institutions investit ce domaine et des fonds considérables sont alloués à cette cause. Pourtant, de multiples initiatives demeurent isolées et sont appliquées en silos – que ce soit en termes de mesures préventives, répressives ou techniques –, empêchant ainsi la **construction et diffusion des connaissances et de bonnes pratique**s. La création d'un réseau européen est une piste de réflexion avancée par certains experts interviewés[271]. À ce sujet, mentionnons le projet de l'Union européenne de créer un centre de compétence européen – semblable à l'organisation NCMEC – pour lutter contre les abus sexuels d'enfants[272]. Un tel centre pourrait également contribuer à améliorer la coopération entre les policiers, les magistrats et les ONG, selon l'un des experts interviewés. Dans cette même logique, une experte suisse interviewés – active dans le domaine de la justice – a soumis l'idée de créer des centres régionaux de compétence pour la poursuite pénale, afin de renforcer davantage la coopération et promouvoir la production de connaissances.

Pour terminer, bien que de nombreuses mesures de prévention soient mises en œuvre, il est difficile de déterminer, d'un point de vue scientifique, quelles démarches sont efficaces et d'établir des bonnes pratiques en la matière. Rares sont les programmes ou les stratégies de prévention de la criminalité à faire l'objet d'une évaluation rigoureuse, et encore plus dans un domaine aussi récent que la cybercriminalité. Ainsi, plusieurs experts interviewés ont mis en évidence le besoin crucial d'allouer des financements pour l'**évaluation scientifique des mesures de prévention** implémentées.

[271] Nous pouvons mentionner le portail européen "Better Internet for Kids" en ce qui concerne l'éducation numérique générale (https://betterinternetforkids.eu).
[272] Nous ne connaissons pas l'état d'avancement du projet. Une procédure de consultation publique avait été ouverte en février 2021.

5. Discussion

En regroupant les informations collectées, nous avons pu saisir une compréhension plus approfondie vis-à-vis des quatre phénomènes de cyberdélinquance sexuelle – la production et la distribution de matériel pédopornographique, le cyber grooming, la sextorsion et le live-streaming – et des mesures de protection des mineurs correspondantes en Suisses et ailleurs. La recherche de littérature a servi de point de départ dans cette étude afin d'établir des connaissances générales sur les phénomènes investigués. La recherche documentaire a permis d'identifier des pratiques en Suisse et dans d'autres pays. Ensuite, les questionnaires remplis par les praticiens ont apporté une perspective plus locale sur les mesures et les collaborations. Enfin, les entretiens avec les experts ont contribué à approfondir certains aspects d'intérêt et à mettre en lumière les challenges, ainsi que des pistes de réflexion en vue d'améliorer les pratiques existantes. Ainsi, dans ce chapitre, nous revenons sur les principales dimensions mises en exergue par cette étude.

Dimension 1 – La connaissance sur les phénomènes : les lacunes sur le cyber grooming, la sextorsion, et le live-streaming

En ce qui concerne la pédopornographie, thématique largement investiguée par la communauté académique, il s'avère que l'attention des chercheurs scientifiques se porte davantage sur la consommation que sur la production ou la distribution de matériel (peut-être en raison d'un accès plus facile aux données). En revanche, le cyber grooming, la sextorsion, et plus particulièrement le live-streaming ont fait l'objet de moins d'études. Il ressort de la présente étude que le live-streaming est peu adressé par les mesures de prévention et reste encore passablement méconnu des acteurs de la prévention.

La recherche de littérature a permis de relever certaines caractéristiques des phénomènes selon les études récentes, notamment en termes de victimes, d'auteurs et de modus operandi en recensant des études menées majoritairement aux Etats-Unis. Au niveau de la Suisse, un manque de données est relevé. Ainsi, de nouvelles recherches sur ces phénomènes permettraient de mieux les connaitre et de concevoir des mesures de prévention en adéquation avec leur évolution.

Dimension 2 – Les acteurs du domaine de la protection des mineurs : une pluralité complexe à coordonner

De manière générale, une pluralité d'acteurs s'est saisie de cette thématique, que ce soit au niveau étatique, associatif, de l'industrie ou encore du milieu scolaire. Néanmoins, une approche en silo est davantage relevée qu'une approche transversale. Mise à part dans le domaine policier où la coopération internationale s'est fortement développée pour lutter contre l'exploitation sexuelle des mineurs sur Internet, des marges d'amélioration subsistent dans les collaborations intra et inter domaine d'activité. Il est ainsi nécessaire de soutenir ce développement en renforçant les réseaux existants qui pourraient agir comme facteur d'harmonisation et de systématisation des connaissances et des compétences.

Dans le domaine policier, la dimension souvent transfrontalière des cyber enquêtes requiert un effort de coordination soutenu entre les polices cantonales et fedpol. Dès lors, des mesures complémentaires

pourraient renforcer les capacités de monitoring et de détection, notamment en harmonisant les bases légales afin de permettre l'échange de données entre corps de police à l'échelle nationale, et en développant des outils de renseignements, de suivi et de détection de situation au sein des polices. D'autre part, le renforcement de partenariats public-privé avec des entreprises ou des institutions permettraient d'obtenir des données complémentaires sur les phénomènes investigués. Un autre exemple de partenariat pourrait prévoir la réception et le triage de matériel pédopornographique par une entreprise privée ou une ONG (comme NCMEC aux Etats-Unis, le Centre canadien de protection de l'enfance au Canada ou l'Internet Watch Foundation au Royaume-Uni) afin de décharger la police en leur transmettant uniquement les contenus illicites.

Enfin, la coopération internationale demeure essentielle pour un suivi efficace de l'évolution de ce phénomène transnational face aux constants changements du panorama numérique. L'accès aux données stockées à l'étranger représente parfois un obstacle dans le cadre des enquêtes policières. Ainsi, une amélioration de la coopération notamment avec les fournisseurs de services étrangers peut contribuer à surmonter cet obstacle. Le deuxième Protocole additionnel à la Convention sur la cybercriminalité[273] va dans ce sens en prévoyant une base légale notamment pour « la coopération directe avec les fournisseurs de services pour les informations sur les abonnés »[274].

Dimension 3 – Les mesures de prévention : une implémentation dissociée et plutôt traditionnelle

La présente étude constate l'implémentation de mesures dissociées qui ne sont pas toujours coordonnées entre elles – dû notamment au fait que les acteurs ne s'organisent pas toujours en réseaux –, ce qui peut générer des incohérences dans les programmes de prévention surtout en raison de la rapide évolution numérique.

De plus, la majorité des mesures identifiées en Suisse prennent la forme de formation (cours de sensibilisation) ou de mise à disposition d'informations et de conseils (sur des sites Internet, en format brochures, etc.). La prévention pourrait dès lors tendre vers des initiatives plus diversifiées alliant divertissement et messages éducatifs, tout en accroissant la présence sur les canaux de communication populaires auprès des groupes cibles (par exemple pour les jeunes, les réseaux sociaux et les plateformes de jeux vidéo). D'autre part, dans le sens de la nouvelle stratégie européenne pour un meilleur Internet pour les enfants (BIK+)[275], les parties prenantes pourraient faire davantage appel aux mineurs ou jeunes adultes (18-25 ans) dans l'élaboration et l'application des mesures de prévention créant ainsi un processus de co-production, et de partage de savoir et d'expériences par les pairs.

Dimension 4 – Le public cible : une approche orientée principalement vers les jeunes et les (potentielles) victimes

La majorité des initiatives de prévention s'adressent principalement aux enfants et aux jeunes, suivie par les mesures destinées aux parents. Il en résulte que la capacité d'action de la prévention se trouve

[273] Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques, STCE n°224.
[274] https://www.coe.int/fr/web/conventions/full-list?module=treaty-detail&treatynum=224
[275] https://ec.europa.eu/commission/presscorner/detail/fr/IP_22_2825

limitée dès lors qu'elle n'inclut pas l'environnement des enfants et des jeunes, à savoir les familles, les enseignants et la communauté au sens large. En ce sens, une approche holistique est à privilégier en développant tant une stratégie de prévention générale destinée à toute la population – et diffusée à large échelle –, qu'une prévention spécifique destinée aux enseignants et tout professionnel du milieu de la jeunesse. Ces groupes de personnes ont une place privilégié dans l'éducation numérique des mineurs et la protection de ces derniers face aux dangers d'Internet, dont les cyber-délits sexuels. Ainsi, les formations et l'échange d'informations sur la thématique des cyber-délits sexuels devraient être encouragés et renforcés auprès de ces groupes afin d'avoir les outils nécessaires pour encadrer et protéger les mineurs.

Enfin, la plupart des mesures de prévention relevées en Suisse (et ailleurs) sont conçues pour les (potentielles) victimes. Néanmoins, il semble pertinent de promouvoir les services existants et de les renforcer pour réduire les conséquences de la victimisation à long terme. D'autre part, la prévention devrait également s'adresser aux (potentiels) auteurs en vue d'empêcher le passage à l'acte ou la récidive. Dans cette perspective de prévention secondaire et tertiaire, le système de soutien et d'aide aux personnes ayant une attirance sexuelle pour les mineurs ou ayant commis un délit sexuel en ligne à l'encontre des mineurs pourrait être renforcé notamment quant au suivi psychologique et au traitement thérapeutique. Ceci implique, d'une part, de promouvoir la formation de thérapeutes spécialisés pour le traitement de (cyber)délinquants sexuels et, d'autre part, d'investiguer si les traitements établis pour les délinquants sexuels correspondent aux besoins des cyberdélinquants sexuels. En effet, il ressort d'un rapport de recherche suisse que les thérapeutes – psychiatres, psychologues et sexologues – sont peu disposés à prendre en charge les personnes attirées sexuellement par des mineurs en raison notamment d'un manque de qualifications[276].

Dimension 5 – L'évaluation des politiques publiques : la difficulté à identifier les bonnes pratiques dans le milieu de la détection et de la prévention

La dispersion des informations relevée dans ce rapport peut également représenter un obstacle dans la compréhension et dans les solutions à proposer pour prévenir et lutter contre les cyber-délits sexuels. Comme observé dans d'autres milieux d'enquête, il y a un besoin de transformer les données en renseignements pour permettre le développement de politiques de lutte plus performantes. Cette approche appelée « Intelligence-led policing » est définie comme un modèle de travail qui recoupe une multitude de données – policières et non policières – pour en extraire les informations utiles et les transformer en renseignements. Le développement d'outils de renseignements, de suivi et de détection de situation permettrait d'améliorer la vision de ces phénomènes et d'optimiser les prises de décisions stratégiques et opérationnelles.

Au-delà de la mise en commun des données existantes, il ressort de l'étude qu'il est difficile d'établir quelles sont les mesures les plus efficaces. En effet, les évaluations scientifiques sur les programmes de prévention en la matière sont très pauvres. De ce fait, la mise en œuvre de processus d'évaluation d'efficacité des programmes de prévention devrait être encouragée et soutenue afin de les perfectionner si nécessaire et de créer du savoir issu des pratiques.

[276] Niehaus et al. (2020).

Sur la base du recensement des mesures implémentées en Suisse et à l'étranger, une typologie de mesures, structurée en huit catégories, a été établie. En comparant les caractéristiques des mesures suisses aux mesures étrangères, et en incorporant les avis relayés par les experts interviewés, nous avons pu dresser un tableau de synthèse des mesures (*infra*, Tab. 14). Celui-ci indique pour chaque catégorie, d'une part, les limites constatées en Suisse et, d'autre part, des pistes de réflexion en vue d'améliorer l'offre des mesures, que ce soit au niveau du public cible, de la communication ou du contenu/format de la mesure.

Tab. 14 – Synthèse sur les mesures préventives et techniques implémentées en Suisse[277]

Activité	Application en Suisse	Pistes de réflexion pour la Suisse
Campagne de sensibilisation nationale	**OUI** Limite : une seule campagne identifiée	• Mettre en œuvre davantage de campagnes nationales • Cibler spécifiquement les cyber-délits, notamment le live-streaming qui demeure peu connu • Impliquer des mineurs dans la conception des campagnes • Utiliser des canaux de communication populaires chez les mineurs • Concevoir ou participer à une campagne internationale • Organiser une journée nationale de sensibilisation
Informations et conseils	**OUI**	• Promouvoir les plateformes auprès des mineurs et des parents, en utilisant les canaux de communication appropriés • Elaborer des guides, destinés aux parents, pour connaître les différents médias utilisés par les mineurs • Concevoir, sur les sites d'informations, une fonction/un bouton de retour instantané vers un site neutre afin de favoriser leur utilisation
Activités ludiques et éducatives	**OUI** Limite : activités plus classiques (livre, jeu de cartes)	• Développer d'autres activités, alliant divertissement, messages éducatifs et canaux de communication préférés par les mineurs (ex. podcast, challenge TikTok, jeu vidéo sérieux) • Promouvoir ces activités sur les canaux de communication préférés des mineurs • Impliquer des mineurs dans la conception des activités
Formation	**OUI** Limites : (1) principalement centrée sur les mineurs, (2) axée plutôt sur la bonne utilisation d'internet de manière générale, (3) orientée prévention de la victimisation	• Renforcer les formations ou soirées informatives pour les parents • Renforcer la formation auprès des enseignants et autres professionnels du milieu de la jeunesse • Aborder davantage les risques liés aux cyber-délits sexuels, notamment sur les jeux vidéo en ligne • Aborder les risques liés aux cyber-délits sexuels plus tôt • Harmoniser les messages clés • Adopter une orientation préventive complémentaire destinée aux (potentiels) auteurs • Impliquer des mineurs dans la conception des activités
Aide et soutien (avec ou sans option de traitement)	**OUI** Limites : (1) peu d'offres pour les (potentiels) auteurs, (2) offres dispersées	• Développer les offres pour les auteurs, notamment en Suisse romande et italienne • Renforcer les offres pour les victimes (par ex. groupe de soutien, permanence juridique dédiée aux abus en ligne sur mineurs) • Concevoir des points d'aide directement sur les plateformes utilisées par les mineurs (réseaux sociaux, jeux vidéo en ligne) • Promouvoir les points d'aide auprès des mineurs, des parents et des professionnels du milieu de la jeunesse
Plateforme de signalement	**OUI**	• Promouvoir les plateformes auprès de la population

[277] Le tableau discute principalement des mesures préventives et techniques. Les mesures policières n'ont pas été introduites dès lors que certains moyens d'investigation ne peuvent pas être publiquement divulgués. Quant aux mesures juridiques, le droit suisse en vigueur criminalise déjà les quatre comportements étudiés dans ce mandat.

	Limite : seul fedpol est habilité au triage des liens URL signalés	• Réaliser une étude sur la pertinence d'habiliter des organisations à recevoir du contenu illicite et effectuer un travail de triage
Logiciel de contrôle / blocage	**OUI**	• Promouvoir ces outils auprès des parents, des professionnels du milieu de la jeunesse, et autres secteurs d'activités concernés, après consultation du cadre légal
Logiciel de détection	**(?)**	• Promouvoir ces outils auprès des secteurs d'activités concernés, après consultation du cadre légal

Note. (?) = La présente étude n'a pas permis d'identifier ce type de mesure en Suisse mais cela ne signifie pas pour autant qu'aucune mesure de ce type est appliquée en Suisse. Certaines informations ont pu échapper aux méthodes de collectes de données.

6. Conclusion et recommandations : réponses aux questions de l'OFAS

Les résultats de l'étude ont permis de répondre comme suit aux questions formulées dans l'appel d'offres de l'OFAS.

1.1a. Où sur Internet et dans quelles situations (types de plateformes et de chats, types d'activités) les différents cyber-délits sexuels ont-ils lieu ?

De manière générale, les plateformes attractives, pour les auteurs de cyber-délits sexuels envers les mineurs, sont les plateformes fréquentées par les jeunes. Et ces plateformes changent au gré de la mode et des avancées technologiques.

L'étude identifie cinq catégories de plateformes :

- **les réseaux sociaux**. Les plus souvent mentionnés sont Instagram, TikTok, Snapchat et Kik. Facebook compte aussi parmi ces plateformes bien que sa popularité semble diminuer au fil des années. Certaines de ces grandes plateformes, comme Instagram et Facebook, ont des mesures de protection et modération (fonction de blocage, possibilité de dénoncer, veille de contenu). De ce fait, ces plateformes sont souvent le point d'accroche avec le mineur, pour ensuite se déplacer sur une plateforme de messagerie cryptée ou retenue comme moins risquée par le pédocriminel.
- **les jeux vidéo en ligne**. Alors qu'elles sont moins sous les projecteurs lors des discours sur les cyber-délits sexuels, les experts rapportent une augmentation de victimisation de mineurs sur ces plateformes (par ex. Fortnite, Minecraft). Tout comme les réseaux sociaux, les plateformes de jeux vidéo contiennent des espaces de discussion et permettent parfois le partage de contenu.
- **les sites réservés aux adultes**. Par exemple, des sites érotiques ou des messageries instantanées pour rencontrer des inconnus (ex. Omegle) où les systèmes de contrôle d'âge ne sont pas souvent sophistiqués.
- **les messageries instantanées** (ex. Telegram, Signal, WhatsApp, Discord), mais d'habitude seulement une fois la discussion bien entamée.
- **le Dark web**. Outre la distribution de pédopornographie, le Dark web permet aux pédocriminels d'échanger sur leurs pratiques et les astuces pour ne pas se faire appréhender. A ce propos, quelques guides du « parfait pédocriminel » seraient en circulation. Il est à relever que des forums de commerce et d'exploitation de mineurs se sont aussi installés sur le Dark web.

1.1b Quelles sont les caractéristiques des victimes et des agresseurs ?

L'avis des experts est qu'il n'y a **pas de profil type au sens strict**. Les affaires de cyber-délits sexuels ont démontré que les victimes et les auteurs proviennent de toutes classes d'âge, de toutes classes sociales, etc. En l'état actuel, les statistiques policières sur la criminalité sexuelle présente une majorité de victimes mineures de sexe féminin et une prédominance de personnes prévenues d'âge adulte et de sexe masculin. Néanmoins, il convient de souligner que les scientifiques ont remarqué un certain nombre de problèmes de représentativité des données policières – celles-ci apportant qu'une

vision partielle de la criminalité réelle – surtout dans le domaine de la délinquance sexuelle. En ce sens, il est délicat de mettre en évidence des caractéristiques, car les informations peuvent être généralisées et mal interprétées, surtout pour des phénomènes plus récents (ex. live-streaming) où les connaissances académiques et des experts, de même que les dénonciations aux autorités policières restent anecdotiques. L'analyse de la littérature académique présente dans le rapport une synthèse détaillée des résultats des études récentes pour chacun des quatre cyber-délits sexuels pris en compte. Néanmoins, plusieurs experts ont évoqué des tendances ou points d'attention relatifs aux quatre phénomènes à l'étude :

- *Production de matériels pédopornographiques* : les experts – suisses et européens – s'accordent sur le fait que depuis quelques années du nouveau matériel – provenant notamment des Etats-Unis – est en circulation, et ce principalement sur le Dark web. Par conséquent, cela signifie que la production est en augmentation. En revanche, sur le territoire helvétique, la production de pédopornographie au sens strict ne semble pas être détectée.
- *Distribution de matériels pédopornographiques* : quant aux méthodes de distribution, la communauté pédocriminelle opère principalement sur le Dark Web. Les méthodes d'échange et de distribution évoluent, dans le sens où le *peer-to-peer* est gentiment abandonné.
- *Cyber grooming* : les activités d'investigation policières indiquent que ce phénomène prend de l'ampleur tant en Suisse romande qu'en France. Pour la Suisse alémanique, les experts interviewés ne se sont pas clairement prononcés, mais présument une augmentation.
- *Sextorsion* : lorsqu'il s'agit de victimes mineures, la sextorsion est employée pour obtenir davantage de matériels pédopornographiques, du nouveau matériel, et du matériel de plus en plus grave.
- *Live-streaming* : ce phénomène est très récent et encore peu connu. Fedpol a tout de même traité un nombre plus élevé de demandes de coordination – de l'étranger vers la Suisse, et de la Suisse vers l'étranger – en matière de live-streaming, ce qui semble alors rejoindre la tendance internationale.

1.2. Quelles mesures existent en Suisse au niveau cantonal, national et international ? Outre les mesures étatiques, les mesures du secteur privé doivent également être incluses (accords d'autorégulation des secteurs, services de plateforme, etc.).

Par le biais des diverses méthodes de collecte de données, le rapport a identifié 86 mesures existantes en Suisse. Plus de la moitié des initiatives identifiées sont implémentées ou rendues accessibles à une échelle cantonale, voire locale. Les initiatives développées dans une perspective nationale représentent un peu plus d'un quart des mesures identifiées. Enfin, d'autres mesures trouvent une portée plus régionale. Conforme à la répartition régionale de la Suisse, les mesures disponibles en Suisse alémanique sont plus nombreuses que les mesures conçues pour la Romandie ou la Suisse italienne.

Les mesures – implémentées en Suisse – traitées dans le cadre de cette étude peuvent être regroupées en quatre catégories :

- **Mesures préventives**. Cette catégorie comprend une campagne de sensibilisation à l'échelle nationale, la mise à disposition d'informations et de conseils sur des plateformes en ligne ou par le biais de brochures, des activités ludiques et éducatives, la formation des jeunes et des

adultes, et des mesures d'aide et soutien (sans option de traitement) visant à soutenir les victimes et leur entourage, ainsi que les (potentiels) auteurs et leurs proches (par ex. des services de permanence, juridiques).

- **Mesures techniques**. Ces mesures prennent la forme de logiciels de contrôle et de blocage, de logiciel de détection, de plateformes de signalements, ainsi que de chartes de sécurité adoptées dans certaines écoles suisses.
- **Mesures policières**. Au niveau de la police, certaines techniques d'enquête et outils sont de nature confidentielle et ne peuvent être divulgués. Peuvent toutefois être mentionnés, le suivi des annonces du National Center for Missing & Exploited Children (NCMEC), le blocage de site Internet, les recherches secrètes préventives, les bases de données de police nationales et internationales, et les collaborations avec d'autres autorités policières/judiciaires étrangères.
- **Mesures juridiques**. Le droit suisse en vigueur criminalise les quatre comportements étudiés dans ce mandat.

1.3a. Qui sont les acteurs et réseaux (par ex. NEDIK) principaux qui proposent des mesures en Suisse ?

Acteurs. L'étude a relevé une pluralité d'acteurs actifs dans divers secteurs : établissements scolaires, autorités étatiques (gouvernements et corps de police), associations et fondations, entreprises privées de télécommunication.

Pour une vision d'ensemble, la figure 1 est disponible au chapitre 4.2.1.

Réseaux. De manière générale, seuls deux groupes de travail et deux réseaux semblent se rapprocher le plus de la thématique à l'étude.

- Le **réseau national de la Prévention suisse de la criminalité (PSC)**, qui réunit les polices cantonales et communales suisses (responsables prévention), fedpol, divers acteurs étatiques et cantonaux, et des ONG.
- Le **réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK)**, créé en 2018 par la Conférence des commandantes et commandants des polices cantonales suisses.
- Le **groupe de travail du Concordat Latin portant sur la cybercriminalité et la lutte contre le pédocriminalité**, regroupant des spécialistes de police des cantons romands et Berne.
- Le **groupe de travail national « sexualité et médias numériques »**, composé de sept associations (Action Innocence, Peer-Campaigns, Pro Juventute, Protection de l'enfance Suisse, SANTE SEXUELLE Suisse, Sexualberatung Bern, Zischtig.ch).

1.3b Quel est leur champ de responsabilité et d'action ?

Ces acteurs s'occupent de traiter les questions liées aux cyber-délits sexuels en fonction de leur champ de responsabilité ou leur domaine d'expertise. Alors que le milieu scolaire contribue principalement

à enseigner une bonne hygiène numérique, les associations et fondations fournissent surtout des conseils et développent des plateformes d'aide et des activités ludiques. En tant que fournisseurs de services de télécommunication, certaines entreprises privées sont impliquées dans la protection des enfants et des jeunes en proposant avant tout des mesures techniques, mais certaines conçoivent aussi des cours de sensibilisation ou financent des études sur l'utilisation des médias. Les départements et offices du gouvernement développent des synergies et des mesures de sensibilisation pour le grand public. Enfin, la police combine un travail répressif en poursuivant la détection et l'investigation des cyber-délits sexuels et un travail de prévention avec des échanges d'informations, des cours de sensibilisation et une présence en ligne tant répressive que préventive.

1.4. À qui s'adressent ces mesures ([potentiels] auteurs du crime, victimes mineures, enfants et jeunes, parents, professionnels, etc.) ?

Les mesures s'adressant aux (potentielles) victimes représentent la majorité. Les mesures qui tendent à modifier l'environnement – situations – et les mesures destinées aux (potentiels) auteurs sont plus rares. En effet, les efforts sont majoritairement concentrés sur la formation des mineurs. Il s'agit principalement des cours de sensibilisation dispensés en milieu scolaire, surtout à un niveau général de bonnes pratiques en termes d'utilisation des médias et des risques inhérents, dont les délits sexuels. Le second type de mesure le plus fréquent est la diffusion d'informations et de conseils. Suivent ensuite les activités ludiques et éducatives, et les mesures d'aide et soutien (sans option de traitement). Enfin, les mesures sous forme de campagnes de sensibilisation à l'échelle nationale sont les moins fréquentes.

Presque la moitié des mesures sont destinées aux jeunes, suivent les mesures adressées aux parents. Peu d'initiatives semblent être formulées pour les enseignants et autres professionnels travaillant avec des enfants et des adolescents.

2.1. Quelles sont les possibilités et les limites de ces mesures ?

Cinq points d'attention ont été mis en exergue dans le cadre de cette étude.

- *Connaissances lacunaires* : un manque de données concernant le cyber grooming, la sextorsion et le live-streaming est relevé, notamment en ce qui concerne les études académiques. En effet, les études recensées sur les quatre phénomènes d'intérêt proviennent majoritairement des pays anglosaxons. Ainsi, un renforcement des recherches, également en Suisse, permettraient de mieux connaitre ces phénomènes et de concevoir des mesures de prévention en adéquation avec leur évolution.
- *Complexité dans la coordination des acteurs* : de manière générale, une pluralité d'acteurs s'est saisie de cette thématique, que ce soit au niveau étatique, associatif, de l'industrie ou encore du milieu scolaire. Néanmoins, une approche en silo est davantage relevée qu'une approche transversale. Mise à part dans le domaine policier où la coopération internationale s'est fortement développée pour lutter contre l'exploitation sexuelle des mineurs sur Internet, des marges d'amélioration subsistent dans les collaborations intra et inter domaine. Il serait ainsi

bénéfique de renforcer les réseaux existants qui pourraient agir comme facteur d'harmonisation et de systématisation des connaissances et des compétences.

- *Mesures dissociées et plutôt traditionnelles* : les mesures sont implémentées sans pour autant être coordonnées entre elles, dû notamment au fait que les acteurs ne s'organisent pas toujours en réseaux. D'autre part, la majorité des mesures identifiées en Suisse prennent la forme de formation (sensibilisation) ou de mise à disposition d'informations et de conseils (sur des sites Internet, brochures, etc.) qui sont des mesures relativement classiques. La prévention pourrait dès lors tendre vers des initiatives plus diversifiées alliant divertissement et messages éducatifs, tout en accroissant la présence sur les canaux de communication populaires auprès des groupes cibles (par ex. pour les jeunes, les réseaux sociaux et les plateformes de jeux vidéo).
- *Approche orientée principalement vers les jeunes et les (potentielles) victimes* : la majorité des initiatives de prévention s'adressent principalement aux enfants et aux jeunes. Or, la capacité d'action de la prévention se trouve limitée dès lors qu'elle n'inclut pas l'ensemble de l'environnement des enfants. En ce sens, une approche holistique est à privilégier. Par ailleurs, la prévention devrait également s'adresser aux (potentiels) auteurs en vue d'empêcher le passage à l'acte ou la récidive. Dans cette perspective de prévention secondaire ou tertiaire, le système de soutien et d'aide (avec et sans option de traitement) aux personnes ayant une attirance sexuelle pour les mineurs ou ayant commis un délit sexuel en ligne à l'encontre des mineurs pourrait être renforcé.
- *Difficulté à identifier les bonnes pratiques dans le milieu de la détection et de la prévention* : la dispersion des informations peut également représenter un obstacle dans la compréhension et dans les solutions à proposer pour prévenir et lutter contre les cyber-délits sexuels. Le développement d'outils de renseignements, de suivi et de détection de situation permettrait d'améliorer la vision de ces phénomènes et d'optimiser les prises de décisions stratégiques et opérationnelles. D'autre part, il ressort de l'étude qu'il est difficile d'établir quelles sont les mesures les plus efficaces. En effet, les évaluations scientifiques sur les programmes de prévention en la matière sont très pauvres. De ce fait, la mise en œuvre de processus d'évaluation d'efficacité des programmes de prévention devrait être encouragée et soutenue afin de les perfectionner si nécessaire et de créer du savoir issu des pratiques.

2.2. Quelles mesures se montrent particulièrement efficaces ? Peut-on identifier des exemples de bonne pratique en Suisse et à l'étranger ? Dans quelle mesure ces dernières peuvent-elles être applicables en Suisse ?

Les experts n'ont pas pu se prononcer à ce sujet, car les évaluations scientifiques sur les programmes de prévention en la matière sont très pauvres. C'est un constat général que l'on peut faire sur les programmes de prévention, et encore plus en lien avec la cybercriminalité qui est un phénomène relativement récent. L'impression est que, dans un cadre d'initiatives dispersées, il demeure difficile de produire de la connaissance sur l'efficacité. Pour la même raison, il est difficile d'identifier des bonnes pratiques. Le tableau 14 (*supra*, ch. 5) offre une synthèse sur les mesures implémentées en Suisse et des pistes de réflexion en vue de les améliorer.

2.3. Dans quelle mesure existe-t-il des lacunes ?

Le rapport a constaté l'existence de lacunes et des marges d'amélioration dans toutes les catégories de mesures investiguées (*supra*, question 2.1). Les recommandations suivantes s'inscrivent dans la logique de combler ces lacunes.

2.4. Quelles recommandations peuvent être formulées pour la Suisse ?

Sur la base des informations recensées dans ce rapport, il est possible de formuler dix recommandations – regroupées sous cinq dimensions – en vue d'améliorer la capacité du système suisse à répondre à ces phénomènes de cyber-délits sexuels à l'encontre des mineurs.

Dimension 1 – La connaissance sur les phénomènes : production du savoir scientifique

Recommandation 1. *Encourager et soutenir les recherches scientifiques sur la thématique des cyber-délits sexuels à l'encontre des mineurs.* Au regard de la revue de littérature, la majorité des études sont menées dans les pays anglosaxons jusqu'à présent, relevant ainsi un manque de données au niveau de la Suisse. De plus, certains phénomènes plutôt récents, comme le live-streaming, sont peu adressés par les mesures de prévention, probablement dû à une méconnaissance de celui-ci. Ainsi, encourager et soutenir de nouvelles recherches scientifiques sur la thématique des cyber-délits sexuels à l'encontre des mineurs (évolution des tendances, caractéristiques auteurs-victimes, modus operandi) permettrait de mieux connaître ces phénomènes et de concevoir des mesures de prévention en adéquation avec leur évolution en Europe.

Dimension 2 – Les acteurs du domaine de la protection des mineurs : renforcement de la coordination

Recommandation 2. *Développer une stratégie nationale pour la prévention des cyber-délits sexuels envers les mineurs.* La plupart des initiatives sont actuellement conçues et/ou appliquées à l'échelle cantonale et locale. Le renforcement de la coordination et de la collaboration entre les diverses parties prenantes (sous l'égide d'une stratégie nationale) permettrait d'harmoniser la prévention et d'obtenir une vision plus exhaustive des pratiques, de leurs forces et faiblesses, et des pistes d'amélioration. La stratégie pourrait prévoir : a) l'activation d'une plateforme de coordination à l'échelle nationale sur les initiatives et les mesures avec tous les acteurs publiques et privés, ainsi qu'une conférence nationale organisée chaque 2-3 ans; b) la définition d'une stratégie de communication et sensibilisation en coordination avec les acteurs déjà actifs pour proposer des campagnes nationales ; c) la constitution d'un observatoire sur les phénomènes en charge de rédiger un rapport annuel.

Recommandation 3. *Renforcer les partenariats public-privé pour le monitoring, le triage et le partage de données.* Des partenariats public-privé pourraient agir comme facteur d'harmonisation et de systématisation des connaissances et des compétences à plusieurs niveaux. En termes de monitoring (suivi systématique des phénomènes), des accords avec des entreprises privées (par ex. fournisseurs de services de télécommunication, entreprises de cybersécurité, ONGs) permettraient d'obtenir des données complémentaires sur les phénomènes investigués. Sur le plan du triage, la réception et le triage de matériel pédopornographique pourraient être

conférés à une entreprise privée ou une ONG (comme NCMEC aux Etats-Unis, le Centre canadien de protection de l'enfance au Canada ou l'Internet Watch Foundation au Royaume-Uni) afin de décharger la police en leur transmettant uniquement les contenus illicites. Quant au partage de données, des partenariats public-privé pourraient être envisagés en vue de trouver un terrain d'entente avec les fournisseurs de services de télécommunication au lieu de passer par la voie de l'entraide juridique qui peut se révéler fastidieuse et de longue durée.

Recommandation 4. *Soutenir l'harmonisation des bases légales pour permettre l'échange de données lors des enquêtes.* Alors que le concordat RBT permet aux corps de police qui en sont membres d'échanger des données, l'équivalent n'est pas observé du côté alémanique. Ainsi, nous recommandons de soutenir les initiatives d'harmonisation des bases légales permettant un tel échange à l'échelle nationale, comme les deux projets en cours de développement que sont l'extension du projet PICSEL – plateforme d'informations de la criminalité sérielle en ligne spécifique à la cybercriminalité – à toutes les polices suisses, et la mise en place de la Plateforme d'interrogation de la police (POLAP).

Dimension 3 – Les mesures de prévention : ouverture à l'innovation

Recommandation 5. *Développer des mesures en alliant divertissement et messages éducatifs, tout en accroissant la présence sur les canaux de communication populaires auprès des groupes cibles (par exemple pour les jeunes, les réseaux sociaux et les plateformes de jeux vidéo).* La majorité des mesures identifiées en Suisse prennent la forme de formation (sensibilisation) ou de mise à disposition d'informations et de conseils (sur des sites Internet, brochures, etc.) qui sont des mesures relativement classiques. Ainsi, des mesures plus diversifiées pourraient être développées (par ex. podcast, challenge TikTok, jeu vidéo sérieux), tout en marquant davantage une présence sur les canaux de communication populaires ou en promouvant les messages de prévention et les services d'aide et soutien.

Recommandation 6. *Octroyer un rôle actif aux mineurs dans la conception et l'application des mesures de prévention (conseil des jeunes, maison de quartier).* Dans le sens de la nouvelle stratégie européenne pour un meilleur Internet pour les enfants (BIK+), les parties prenantes pourraient faire davantage appel à des mineurs ou jeunes adultes (18-25 ans) dans la conception et l'application des mesures de prévention créant ainsi un processus de co-production, et de partage de savoir et d'expériences par les pairs.

Dimension 4 – Le public cible : inclusion à travers une approche holistique

Recommandation 7. *Renforcer la formation des enseignants et des professionnels du milieu de la jeunesse*. La majorité des initiatives de prévention s'adressent principalement aux enfants et aux jeunes, suivie ensuite par celles destinées aux parents. En revanche, nous relevons que peu d'initiatives sont formulées pour les enseignants et autres professionnels travaillant avec des enfants et des adolescents. Il en résulte que la capacité d'action de la prévention se trouve limitée dès lors qu'elle n'inclut pas l'ensemble de l'environnement des enfants et des jeunes. En ce sens, une approche holistique est à privilégier en développant notamment une prévention spécifique destinée aux enseignants et tout professionnel du milieu de la jeunesse. Ces groupes de personnes ont une place privilégié dans l'éducation numérique des mineurs et la protection de ces derniers

face aux dangers d'Internet, dont les cyber-délits sexuels. Ainsi, les formations et l'échange d'informations sur la thématique des cyber-délits sexuels devraient être encouragés et renforcés auprès de ces groupes afin d'avoir les outils nécessaires pour encadrer et protéger les mineurs.

Recommandation 8. *Soutenir le développement et la promotion d'un réseau de soutien et d'aide (avec et sans option de traitement) pour les victimes et les (potentiels) auteurs.* La plupart des mesures de prévention relevées en Suisse (et ailleurs) sont conçues pour les (potentielles) victimes. Néanmoins, il semble pertinent de promouvoir les services existants et de les renforcer pour réduire les conséquences de la victimisation à long terme. D'autre part, la prévention devrait également s'adresser aux (potentiels) auteurs en vue d'empêcher le passage à l'acte ou la récidive. Dans cette perspective de prévention secondaire et tertiaire, un réseau de soutien et d'aide (avec et sans option de traitement) aux personnes ayant une attirance sexuelle pour les mineurs ou ayant commis un délit sexuel en ligne à l'encontre des mineurs pourrait être renforcé notamment quant au suivi psychologique et au traitement thérapeutique. Ceci implique, d'une part, de promouvoir la formation de thérapeutes spécialisés pour le traitement de (cyber)délinquants sexuels et, d'autre part, d'investiguer si les traitements établis pour les délinquants sexuels correspondent aux besoins des cyberdélinquants sexuels.

Dimension 5 – L'évaluation des politiques publiques : production du savoir issu de la pratique (evidence-based)

Recommandation 9. *Développer des outils de renseignements, de suivi et de détection de situation.* Comme observé dans d'autres milieux d'enquête, il y a un besoin de transformer les données en renseignements pour permettre le développement des politiques de lutte plus performantes. Cette approche appelée « Intelligence-led policing » est définie comme un modèle de travail qui recoupe une multitude de données – policières et non policières – pour en extraire les informations utiles et les transformer en renseignements. Le développement d'outils de renseignements, de suivi (monitoring) et de détection de situation – comme la plateforme PICSEL – permettrait d'améliorer la vision de ces phénomènes et d'optimiser les prises de décisions stratégiques et opérationnelles.

Recommandation 10. *Encourager et soutenir l'évaluation scientifique de programmes de prévention.* Il ressort de l'étude qu'il est difficile d'établir, d'un point de vue scientifique, quelles sont les mesures les plus efficaces. En effet, les évaluations sur les programmes de prévention de la criminalité sont pauvres, et encore plus dans un domaine aussi récent que la cybercriminalité. De ce fait, la mise en œuvre de processus d'évaluation d'efficacité des programmes de prévention devrait être encouragée et soutenue afin de les perfectionner si nécessaire et de créer du savoir issu des pratiques.

7. Glossaire

Auteur mixte : Par consommateurs de pédopornographie, la littérature recensée les différencie des auteurs mixtes qui consomment de la pédopornographie en plus de commettre des actes d'ordre sexuel sur enfants.

Chatbox : Boîte de dialogue permettant d'entrer en communication avec d'autres personnes en ligne.

Chat room : Un emplacement sur Internet où des utilisateurs peuvent s'échanger des messages, généralement sur un sujet spécifique.[278]

Clear web : Espace web suivant la régulation de l'ICANN dont l'IP de la ressource est visible. Certaines ressources du « clear web » sont indexées par des moteurs de recherche (ex. Google).[279]

Cyber grooming : également appelé pédopiégeage, ce comportement consiste à entrer en contact avec un enfant sur Internet à des fins sexuelles.

Dark web : Espace web autorégulé utilisant l'infrastructure d'Internet dont l'adresse IP de la ressource (ex. site web) n'est pas visible. Pour accéder au « dark web », il faut utiliser des logiciels spécifiques (ex. Tor browser).[280]

IRC (Internet Relay Chat) : Internet Relay Chat est un protocole de communication. Les utilisateurs se connectent sur un serveur, puis ils peuvent s'échanger des messages ou des fichiers.

Live-streaming d'actes d'ordre sexuel : ce comportement consiste à diffuser en direct des actes d'ordre sexuel effectués par l'enfant lui-même ou par une personne tierce sur l'enfant.

Même : Élément de langage reconnaissable et transmis par répétition d'un individu à l'autre. Sur Internet, il s'agit le plus souvent d'une image, d'une musique ou d'une vidéo reprise et déclinée en masse dans un but humoristique.

Newsgroup : Groupe de discussion établi sur un USENET (système de réseau de forums inventé avant l'arrive du web). Il est possible de se connecter à certains USENET en utilisant des logiciels ou plateformes spécifiques (ex. https://groups.google.com/).

Nude : Un nude est une photo de soi-même qu'on prend avec son smartphone, en étant nu ou partiellement dénudé. Autrement dit, c'est un selfie nu. Dans certains cas, une telle photo est destinée à être envoyée à un destinataire. Ce mot s'emploie le plus souvent au pluriel : des nudes. Il peut aussi désigner une photo d'un modèle nu prise par un photographe.[281]

Podcast : Émissions, le plus souvent au format audio, qui sont diffusées et peuvent être écoutées en ligne.

Prévention primaire – secondaire – tertiaire : La prévention de la criminalité comprend toute activité individuelle ou de groupe, publique ou privée, visant à éliminer les infractions avant qu'elles se produisent ou avant que toute activité supplémentaire n'en résulte. En s'inspirant du modèle de santé publique, certains théoriciens ont établi une distinction entre prévention primaire (universelle),

[278] https://dictionary.cambridge.org/fr/dictionnaire/anglais/chat-room
[279] https://www.zdnet.com/pictures/a-basic-guide-to-the-deep-dark-web/
[280] https://www.kaspersky.fr/resourcecenter/threats/deep-web
[281] https://dictionnaire.orthodidacte.com/article/definition-nude

prévention secondaire (personnes à risque de délinquance ou de victimisation) et prévention tertiaire (délinquants avérés, victimes avérées).[282]

Prévention situationnelle – sociale : La prévention situationnelle comprend des mesures de réduction des opportunités qui (1) visent des formes de criminalité très spécifiques, (2) qui impliquent la gestion, la conception ou la manipulation de l'environnement immédiat de manière aussi spécifique et permanente que possible, (3) afin de rendre la commission d'infractions plus difficile et plus risquée, tout en réduisant les avantages qu'un large éventail de personnes délinquantes pourrait en attendre. La prévention sociale s'attache à éliminer les problèmes qui peuvent entraîner une personne vers la criminalité, tels que les carences de l'encadrement parental pour les jeunes, une mauvaise éducation primaire ou une piètre santé physique ou mentale. La communauté apporte son aide en enseignant le respect de la loi, en forgeant des relations entre la police et la communauté locales et en établissant des centres d'accueil et d'aide pour la population.[283]

Production ou distribution de matériel pédopornographique via Internet : ce comportement inclut notamment les représentations de contenus sexuels, focalisées sur les organes sexuels d'un enfant et ayant pour but de susciter une excitation sexuelle.

Réseau pair-à-pair : Se dit du mode d'utilisation d'un réseau dans lequel chacun des participants connectés dispose des mêmes droits et qui permet un échange direct de services sans recourir à un serveur central.[284]

Sextorsion : ce comportement consiste à faire chanter l'enfant suite à l'acquisition de matériel numérique de type sexuel, comme le fait de se procurer des photos osées d'un mineur au travers de réseaux sociaux.

TIC (Technologies de l'information et de la communication) : Les technologies de l'information et de la communication désignent autant les appareils, les réseaux que des logiciels informatiques.

TikTok : Application mobile de partage de vidéo et de réseautage social.

Tor : Réseau mondial décentralisé de routeurs, organisés en couches, appelés nœuds de l'oignon, dont la tâche est de transmettre de manière anonyme des paquets TCP (Transmission Control Protocol). C'est ainsi que tout échange Internet basé sur TCP peut être rendu anonyme en utilisant Tor. C'est un logiciel libre distribué sous licence BSD (Berkeley Software Distribution License) révisée.[285]

WhatsApp : Application mobile avec un système de messagerie instantanée permettant d'entrer en communication avec des numéros connus.

[282] https://www.unodc.org/e4j/fr/crime-prevention-criminal-justice/module-2/key-issues/1--definition-of-crime-prevention.html
[283] https://www.unodc.org/e4j/fr/crime-prevention-criminal-justice/module-2/key-issues/2a--detailed-explanation-of-tonry-and-farringtons-typology.html
[284] http://www.culture.fr/franceterme/terme/INFO909
[285] https://techno-science.net

8. Bibliographie

Aebi, M. F. (2006). *Comment mesurer la délinquance ?* : Armand Colin.

Aebi, M. F., Caneppele, S., & Molnar, L. (2022). *Measuring Cybercrime in Europe: The Role of Crime Statistics and Victimisation Surveys. Proceedings of a Conference Organised by the Council of Europe with the Support of the European Union, 29-30 October 2020*: Eleven.

Ali, S., Haykal, H. A., & Youssef, E. Y. M. (2021). Child Sexual Abuse and the Internet—A Systematic Review. *Human Arenas*, 1-18. doi:10.1007/s42087-021-00228-9

Armstrong, J., & Mellor, D. (2016). Internet child pornography offenders: An examination of attachment and intimacy deficits. *Legal and Criminological Psychology, 21*(1), 41-55. doi:10.1111/lcrp.12028

asut. (2021). *Initiative sectorielle de l'asut pour la protection de la jeunesse face aux médias. Edition juin 2021*. Association Suisse des Télécommunications. Berne. Consulté à https://asut.ch/asut/media/id/2264/type/document/Initiative+sectorielle+pour+la+protection+de+la+jeunesse+face+aux+m%C3%A9dias+2021.pdf

Baier, D. (2019). *Kriminalitätsopfererfahrungen und Kriminalitätswahrnehmungen in der Schweiz Ergebnisse einer Befragung*. Institute of Delinquency and Crime Prention, University of Applied Sciences. Zurich

Bale, H. L. (2017). *Online child sexual offending: psychological characteristics of offenders and the process of exploitation.* (phdthesis), University of Edinburgh, era.ed.ac.uk database.

Bartels, R. M., & Merdian, H. L. (2016). The implicit theories of child sexual exploitation material users: An initial conceptualization. *Aggression and Violent Behavior, 26*, 16-25. doi:10.1016/j.avb.2015.11.002

Bernath, J., Suter, L., Walter, G., Külling, C., Willemse, I., & Süss, D. (2020). *JAMES - Jeunes, activités, médias - enquête Suisse*. Zürcher Hochscule für Angewandte Wissenschften. Zurich

Bickart, W., McLearen, A. M., Grady, M. D., & Stoler, K. (2019). A descriptive study of psychosocial characteristics and offense patterns in females with online child pornography offenses. *Psychiatry, Psychology and Law, 26*(2), 295-311. doi:10.1080/13218719.2018.1506714

Bissias, G., Levine, B., Liberatore, M., Lynn, B., Moore, J., Wallach, H., & Wolak, J. (2016). Characterization of contact offenders and child exploitation material trafficking on five peer-to-peer networks. *Child Abuse & Neglect, 52*, 185-199. doi:10.1016/j.chiabu.2015.10.022

Boxall, H., Pooley, K., Franks, C., Long, C., & Dowling, C. (2021). Patterns and predictors of reoffending among child sexual offenders: A rapid evidence assessment. *Trends and Issues in Crime and Criminal Justice*(632), 1-19. doi:10.3316/INFORMIT.20211101056190

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime prevention: Theory and applications*: Springer.

Briggs, P., Simon, W. T., & Simonsen, S. (2011). An Exploratory Study of Internet-Initiated Sexual Offenses and the Chat Room Sex Offender: Has the Internet Enabled a New Typology of Sex Offender? *Sexual Abuse, 23*(1), 72-91. doi:10.1177/1079063210384275

Broome, L. J., Izura, C., & Davies, J. (2020). A psycho-linguistic profile of online grooming conversations: A comparative study of prison and police staff considerations. *Child Abuse & Neglect, 109*, 434-444. doi:10.1016/j.chiabu.2020.104647

Brown, R., & Bricknell, S. (2018). What is the profile of child exploitation material offenders? *Trends and Issues in Crime and Criminal Justice*(564), 1-14. doi:10.3316/informit.045842814111758

Burkhardt, C., da Silva, A., & Caneppele, S. (2020). *Criminal Justice, Legal Framework and Prevention Policies in relation to juvenile cybercrime.* University of Lausanne

Cale, J., Holt, T., Leclerc, B., Singh, S., & Drew, J. (2021). Crime commission processes in child sexual abuse material production and distribution: A systematic review. *Trends and Issues in Crime and Criminal Justice*(617), 1-22. doi:10.3316/informit.721282335565713

Cambi Favre-Bulle, A. (2017). Art. 197 CP. In A. Macaluso, L. Moreillon, & N. Queloz (Eds.), *Commentaire romand Code pénal II art. 111-392 CP*: Helbing Lichtenhahn.

Caneppele, S., & Aebi, M. F. (2019). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice, 13*(1).

Caneppele, S., Milani, R., Burkhardt, C., da Silva, A., & Aebi, M. F. (2019). *La sicurezza a Lugano nel 2019: 4. Nuove tecnologie e vittimizzazione online*

Charles, A. T. (2017). *The abuse of teenagers by online predators facilitated through the Internet and social media.* (mastersthesis), Utica College, Ann Arbor, United States. ProQuest database.

Chiu, M. M., Seigfried-Spellar, K. C., & Ringenberg, T. R. (2018). Exploring detection of contact vs. fantasy online sexual offenders in chats with minors: Statistical discourse analysis of self-disclosure and emotion words. *Child Abuse & Neglect, 81*, 128-138. doi:10.1016/j.chiabu.2018.04.004

Christensen, L. S., & Tsagaris, G. S. (2020). Offenders convicted of child sexual exploitation material offences: characteristics of offenders and an exploration of judicial censure. *Psychiatry, Psychology and Law, 27*(4), 647-664. doi:10.1080/13218719.2020.1742240

Clevenger, S. L., Navarro, J. N., & Gilliam, M. (2018). Technology and the endless "cat and mouse" game: A review of the interpersonal cybervictimization literature. *Sociology Compass, 12*(12), 1-13. doi:10.1111/soc4.12639

Clevenger, S. L., Navarro, J. N., & Jasinski, J. L. (2016). A matter of low self-control? Exploring differences between child pornography possessors and child pornography producers/distributers using self-control theory. *Sexual Abuse, 28*(6), 555-571. doi:10.1177/1079063214557173

Commission de la politique de sécurité du Conseil des États. (2019). *Mo. Conseil national (Eichenberger). Échange de données de police au niveau national. Rapport de la Commission de la politique de sécurité du 10 octobre 2019*.

Commission des affaires juridiques du Conseil des États. (2022). *Harmonisation des peines et adaptation du droit pénal accessoire au nouveau droit des sanctions. Projet 3 : loi fédérale portant révision du droit pénal en matière sexuelle. Rapport de la Commission des affaires juridiques du Conseil des États*.

Conférence des directrices et directeurs des départements cantonaux de justice et police. (2020). Communiqué de presse du 17 novembre 2020 : Renforcement des efforts cantonaux contre la cybercriminalité et la pédocriminalité. Consulté à https://www.kkjpd.ch/newsreader-fr/renforcement-des-efforts-cantonaux-contre-la-cybercri-minalit%C3%A9-et-la-p%C3%A9docriminalit%C3%A9.html?file=files/Dokumente/News/2020/201117%20Communique%20de%20presse%20NEDIK.pdf

Conseil fédéral. (2018). *Stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022*. Confédération suisse

Conseil fédéral. (2020a). *Offres de prévention destinées aux personnes attirées sexuellement par les enfants. Rapport du Conseil fédéral en réponse aux postulats Rickli Natalie 16.3637 et Jositsch Daniel 16.3644 du 12 septembre 2016 « Mise en place en Suisse d'un projet de prévention du type Kein Täter werden »*. Berne

Conseil fédéral. (2020b). *Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018–2022. État au premier trimestre 2020*.

Conseil fédéral. (2022). *Harmonisation des peines et adaptation du droit pénal accessoire au nouveau droit des sanctions. Projet 3: loi fédérale portant révision du droit pénal en matière sexuelle. Rapport du 17 février 2022 de la Commission des affaires juridiques du Conseil des États. Avis du Conseil fédéral*. FF 2022 1011

Conseil fédéral, & Secrétariat général DFF. (2022). Communiqué de presse du 18 mai 2022: Le Centre national pour la cybersécurité deviendra un office fédéral. Consulté à https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/medienmitteilungen/newslist.msg-id-88878.html

Corboz, B. (2010). *Les infractions en droit suisse* (3 ed. Vol. 1). Berne: Stämpfli.

Côté, A.-M., Bérubé, M., & Dupont, B. (2016). "Statistiques et menaces numériques: Comment les organisations de sécurité quantifient la cybercriminalité". *Réseaux, 197-198*(3).

Cubitt, T., & Napier, S. (2021). *Predicting prolific live streaming of child sexual abuse* (634). Australian Institute of Criminology. Australia

da Silva, A., Burkhardt, C., & Caneppele, S. (2022). Challenges in measurement of cybercrime. Consulté à https://www.ccdriver-h2020.com/_files/ugd/0ef83d_5612d75012b64b6e993c0fd9368ed36b.pdf

Davis, N. (2016). *Improving practice in Child Sexual Abuse Image and Grooming investigations through identification of offender characteristics.* (phdthesis), Charles Suart University, researchoutput.csu.edu.au database.

de Santisteban, P., del Hoyo, J., Alcázar-Córcoles, M. Á., & Gámez-Guadix, M. (2018). Progression, maintenance, and feedback of online child sexual grooming: A qualitative analysis of online predators. *Child Abuse & Neglect, 80*, 203-215. doi:10.1016/j.chiabu.2018.03.026

de Santisteban, P., & Gámez-Guadix, M. (2018). Longitudinal and reciprocal relationships of depression among minors with online sexual solicitations and interactions with adults. *Cyberpsychology, Behavior, and Social Networking, 21*(6), 355-360. doi:10.1089/cyber.2017.0641

DeHart, D., Dwyer, G., Seto, M. C., Moran, R., Letourneau, E., & Schwarz-Watts, D. (2017). Internet sexual solicitation of children: a proposed typology of offenders based on their chats, e-mails, and social network posts. *Journal of Sexual Aggression, 23*(1), 77-89. doi:10.1080/13552600.2016.1241309

DeMarco, J., Cheevers, C., Davidson, J., Bogaerts, S., Pace, U., Aiken, M., Caretti, V., Schimmenti, A., & Bifulco, A. (2017). Digital dangers and cyber-victimisation: a study of European adolescent online risky behaviour for sexual exploitation. *Clinical Neuropsychiatry, 14*(1), 104-112.

DeMarco, J., Sharrock, S., Crowther, T., & Barnard, M. (2018). *Behavior and characteristics of perpetrators of online-facilitated child sexual abuse and exploitation*. Prepared for Independent Inquiry into Child Sexual Abuse (IICSA)

Drouin, M., Boyd, R. L., & Greidanus Romaneli, M. (2018). Predicting recidivism among internet child sex sting offenders using psychological language analysis. *Cyberpsychology, Behavior, and Social Networking, 21*(2), 78-83. doi:10.1089/cyber.2016.0617

Drouin, M., Boyd, R. L., Hancock, J. T., & James, A. (2017). Linguistic analysis of chat transcripts from child predator undercover sex stings. *The Journal of Forensic Psychiatry & Psychology, 28*(4), 437-457. doi:10.1080/14789949.2017.1291707

Elbert, M. J., Drury, A. J., & DeLisi, M. (2021). Child pornography possession/receipt offenders: Developing a forensic profile. *Psychiatry, Psychology and Law, 0*(0), 1-14. doi:10.1080/13218719.2021.1904447

EUROPOL. (2020). *EXPLOITING ISOLATION: Offenders and victims of online child sexual abuse during the COVID-19 pandemic*. European Union Agency for Law Enforcement Cooperation. Consulté à https://www.europol.europa.eu/publications-documents/exploiting-isolationoffenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic

Forni, G., Pietronigro, A., Tiwana, N., Gandolfi, N., Del Castillo, C. E., Mosillo, G., & Pellais, A. (2020). Little red riding hood in the social forest. Online grooming as a public health issue: A narrative review. *Annali di igiene: medicina preventiva e di comunita, 32*(3), 305-318. doi:10.7416/ai.2020.2353

Fortin, F., Paquette, S., & Dupont, B. (2017). De la pornographie légale à l'agression sexuelle : les scripts des activités des cyberdélinquants sexuels. *Criminologie, 50*(1), 203-231. doi:10.7202/1039802ar

Fortin, F., Paquette, S., & Dupont, B. (2018). From online to offline sexual offending: Episodes and obstacles. *Aggression and Violent Behavior, 39*, 33-41. doi:10.1016/j.avb.2018.01.003

Fortin, F., & Proulx, J. (2019). Sexual interests of child sexual exploitation material (CSEM) consumers: Four patterns of severity over time. *International Journal of Offender Therapy and Comparative Criminology, 63*(1), 55-76. doi:10.1177/0306624X18794135

Gámez-Guadix, M., Almendros, C., Calvete, E., & De Santisteban, P. (2018). Persuasion strategies and sexual solicitations and interactions in online sexual grooming of adolescents: Modeling direct and indirect pathways. *Journal of Adolescence, 63*, 11-18. doi:10.1016/j.adolescence.2017.12.002

Gercke, M. (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. ITU Telecommunication Development Sector. Consulté à http://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Gewirtz-Meydan, A., Walsh, W., Wolak, J., & Finkelhor, D. (2018). The complex experience of child pornography survivors. *Child Abuse & Neglect, 80*, 238-248. doi:10.1016/j.chiabu.2018.03.031

Goller, A., Jones, R., Dittmann, V., Taylor, P., & Graf, M. (2016). Criminal recidivism of illegal pornography offenders in the overall population - a national cohort study of 4612 offenders in Switzerland. *Advances in Applied Sociology, 6*(2), 48-56. doi:10.4236/aasoci.2016.62005

Gottfried, E. D., Shier, E. K., & Mulay, A. L. (2020). Child pornography and online sexual solicitation. *Current Psychiatry Reports, 22*(3), 10. doi:10.1007/s11920-020-1132-y

Henshaw, M. (2017). *The demographic, mental health and offending characteristics of online child pornography offenders: a comparison with contact-only and dual sexual offenders.* (PhD Thesis), Swinburne University of Technology, researchbank.swinburne.edu.au database.

Henshaw, M., Arnold, C., Darjee, R., Ogloff, J. R., & Clough, J. A. (2020). Enhancing evidence-based treatment of child sexual abuse material offenders: The development of the CEM-COPE program. *Trends and Issues in Crime and Criminal Justice*(607), 1-14. doi:10.3316/agispt.20201215041192

Henshaw, M., Ogloff, J. R. P., & Clough, J. A. (2017). Looking beyond the screen: A critical review of the literature on the online child pornography offender. *Sexual Abuse, 29*(5), 416-445. doi:10.1177/1079063215603690

Hermida, M. (2019). *EU Kids Online Suisse. Les enfants et les jeunes suisses sur Internet : risques et opportunités. Extrait des résultats*. Haute école pédagogique de Schwyz. Goldau

Hirsig-Vouilloz, M. (2021). Art. 69 CP. In L. Moreillon, A. Macaluso, N. Queloz, & N. Dongois (Eds.), *Commentaire romand Code pénal I art. 1-110 CP*

(2ème ed.). Bâle: Helbing Lichtenhahn.

Ioannou, M., Synnott, J., Reynolds, A., & Pearson, J. (2018). A comparison of online and offline grooming characteristics: An application of the victim roles model. *Computers in Human Behavior, 85*, 291-297. doi:10.1016/j.chb.2018.04.011

Joleby, M., Lunde, C., Landström, S., & Jonsson, L. S. (2020). "All of me is completely different": Experiences and consequences among victims of technology-assisted child sexual abuse. *Frontiers in Psychology, 11*, 3432. doi:10.3389/fpsyg.2020.606218

Joleby, M., Lunde, C., Landström, S., & Jonsson, L. S. (2021). Offender strategies for engaging children in online sexual activity. *Child Abuse & Neglect, 120*, 105214. doi:10.1016/j.chiabu.2021.105214

Kleijn, M., & Bogaerts, S. (2020). Sexual offending pathways and chat conversations in an online environment. *Sexual Abuse*, 1079063220981061. doi:10.1177/1079063220981061

Kloess, J. A., Hamilton-Giachritsis, C. E., & Beech, A. R. (2017). A descriptive account of victims' behaviour and responses in sexually exploitative interactions with offenders. *Psychology, Crime & Law, 23*(7), 621-632. doi:10.1080/1068316X.2017.1293052

Kopecký, K. (2017). Online blackmail of Czech children focused on so-called "sextortion" (analysis of culprit and victim behaviors). *Telematics and Informatics, 34*(1), 11-19. doi:10.1016/j.tele.2016.04.004

Krone, T. (2004). A typology of online child pornography offending Typology of child pornography offending Australia. *Trends & issues in crime and criminal justice*(279), 1-6.

Krone, T., Smith, R. G., Cartwright, J., Hutchings, A., Tomison, A., & Napier, S. (2017). *Online child sexual exploitation offenders: A study of Australian law enforcement data* (1213)

Laajasalo, T., Ellonen, N., Korkman, J., Pakkanen, T., & Aaltonen, O.-P. (2020). Low recidivism rates of child sex offenders in a Finnish 7-year follow-up. *Nordic Journal of Criminology, 21*(1), 103-111. doi:10.1080/2578983X.2020.1730069

Lacasse, L. (2017). *Consommateurs de pornographie juvénile et agresseurs sexuels, du pareil au même? Comparaisons sur le plan développemental et comportemental.* (mastersthesis), University of Montreal, papyrus.bib.umontreal.ca database.

Lamothe, J.-O. (2020). *Les facteurs de risque dynamiques associés à l'agression sexuelle chez les cyberdélinquants.* (mastersthesis), University of Montreal, papyrus.bib.umontreal.ca database.

Leclerc, B., Drew, J., Holt, T., Cale, J., & Singh, S. (2021). *Child sexual abuse material on the darknet: a script analysis of how offenders operate*. Australian Institute of Criminology

Lightfoot, J. W. (2016). *Law enforcements perceptions and preparedness to address child exploitation via hacking.* (mastersthesis), Georgia Southern University, digitalcommons.georgiasouthern.edu database.

Lorenzo-Dus, N., & Izura, C. (2017). "cause ur special": Understanding trust and complimenting behaviour in online grooming discourse. *Journal of Pragmatics, 112*, 68-82. doi:10.1016/j.pragma.2017.01.004

Lorenzo-Dus, N., Izura, C., & Pérez-Tattam, R. (2016). Understanding grooming discourse in computer-mediated environments. *Discourse, Context & Media, 12*, 40-50. doi:10.1016/j.dcm.2016.02.004

Ly, T., Dwyer, R. G., & Fedoroff, J. P. (2018). Characteristics and treatment of internet child pornography offenders. *Behavioral Sciences & the Law, 36*(2), 216-234. doi:10.1002/bsl.2340

Machimbarrena, J. M., Calvete, E., Fernández-González, L., Álvarez-Bardón, A., Álvarez-Fernández, L., & González-Cabrera, J. (2018). Internet risks: An overview of victimization in cyberbullying, cyber dating abuse, sexting, online grooming and problematic Internet use. *International Journal of Environmental Research and Public Health, 15*(11), 2471. doi:10.3390/ijerph15112471

Massicotte, F. (2016). *Analyse quantitative de la carrière criminelle des internautes effectuant du leurre d'enfants.* (mastersthesis), University of Montreal, papyrus.bib.umontreal.ca database.

McGuire, M., & Dowling, S. (2013). *Cybercrime: A review of the evidence: Summary of key findings and implications*. Home Office. London. Consulté à https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

Merdian, H. L., Moghaddam, N., Boer, D. P., Wilson, N., Thakker, J., Curtis, C., & Dawson, D. (2018). Fantasy-driven versus contact-driven users of child sexual exploitation material: Offender classification and implications for their risk assessment. *Sexual Abuse, 30*(3), 230-253. doi:10.1177/1079063216641109

Meyer, P. (2020). *Sollicitation d'enfants à des fins sexuelles en ligne : lacunes légales et solutions en Suisse.* (Mémoire de Master en Droit),

Molina Martinez, G. (2019). *Typologie des cas d'échange d'images sexuelles produites par les jeunes par le biais d'Internet : une étude exploratoire chez les adolescentes âgées de moins de 18 ans.* (mastersthesis), University of Montreal, papyrus.bib.umontreal.ca database.

Napier, S., Brown, R., & Smith, R. G. (2020). Australians who view live streaming of child sexual abuse: An analysis of financial transactions. *Trends and Issues in Crime and Criminal Justice*(589), 1-16. doi:10.3316/agispt.20200415028654

Napier, S., Teunissen, C., & Boxall, H. (2021). Live streaming of child sexual abuse: An analysis of offender chat logs Live streaming of child sexual abuse. *Trends & Issues in Crime & Criminal Justice*(639), 1-15.

Newton, A. L. (2021). *An evaluation of the rise of online sexual exploitation of children and technology: How the past three decades speak to future.* (PhD Thesis), baylor-ir.tdl.org database.

Niehaus, S., Pisoni, D., & Schmidt, A. F. (2020). *Präventionsangebote für Personen mit sexuellen Interessen an Kindern und ihre Wirkung*. Bundesamt für Sozialversicherungen. Bern

Nikolovska, M. (2020). *The Internet as a creator of a criminal mind and child vulnerabilities in the cyber grooming of children.* University of Jyväskylä,

O'Malley, R. L., & Holt, K. M. (2020). Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. *Journal of Interpersonal Violence*, 0886260520909186. doi:10.1177/0886260520909186

Owen, T., Noble, W., & Speed, F. C. (2017). Cyber Grooming: How Biological Variables Reinforce Cognitive Distortion. In T. Owen, W. Noble, & F. C. Speed (Eds.), *New Perspectives on Cybercrime* (pp. 81-111). Cham: Springer International Publishing.

Owens, J. N., Eakin, J. D., Hoffer, T., Muirhead, Y., & Shelton, J. L. E. (2016). Investigative aspects of crossover offending from a sample of FBI online child sexual exploitation cases. *Aggression and Violent Behavior, 30*, 3-14. doi:10.1016/j.avb.2016.07.001

Paquette, S. (2019). *Les cognitions soutenant la cyberdélinquance sexuelle commise envers les enfants : leur nature, leur mesure et leur rôle.* (phdthesis), University of Montreal, papyrus.bib.umontreal.ca database.

Paquette, S. (2022). *« COGNITIONS ET ÉMOTIONS PROBLÉMATIQUES CHEZ LES CYBERDÉLINQUANTS SEXUELS : MISE À JOUR DES CONNAISSANCES ET OUTILS D'ÉVALUATION »*. Paper presented at the Conférence-midi FORENSIA - Centre de formation en santé mentale justice et sécurité (PINEL), En ligne.

Paquette, S., & Cortoni, F. (2021). Offence-supportive cognitions, atypical sexuality, problematic self-regulation, and perceived anonymity among online and contact sexual offenders against children. *Archives of Sexual Behavior, 50*(5), 2173-2187. doi:10.1007/s10508-020-01863-z

Patchin, J. W., & Hinduja, S. (2020). Sextortion among adolescents: Results from a national survey of U.S. youth. *Sexual Abuse, 32*(1), 30-54. doi:10.1177/1079063218800469

Pedrazzini Rizzi, V. (2017). Art. 196. In A. Macaluso, L. Moreillon, & N. Queloz (Eds.), *Commentaire romand Code pénal II art. 111-392 CP*: Helbing Lichtenhahn.

Petitpierre, M. (2014). *Projet pilote de jeu vidéo sérieux sur la protection des jeunes et leur image numérique. Une analyse de son processus d'élaboration et son évaluation.* (Mémoire de Master), Université de Lausanne, Lausanne.

Pugnière-Saavedra, F. (2018). Un usage déviant du numérique : le cas des détenteurs et des diffuseurs de vidéos pédopornographiques sur internet. *Terminal. Technologie de l'information, culture & société*(123). doi:10.4000/terminal.3317

Quayle, E. (2017). *Over the Internet, under the eadar: Online child sexual abuse and exploitation – a brief literature review*. Center for youth and criminal justice. Scotland

Quayle, E., Jonsson, L. S., Cooper, K., Traynor, J., & Svedin, C. G. (2018). Children in identified sexual images – Who are they? Self- and non-self-taken images in the International child

sexual exploitation image database 2006–2015. *Child Abuse Review, 27*(3), 223-238. doi:10.1002/car.2507

Quayle, E., & Newman, E. (2016). An exploratory study of public reports to investigate patterns and themes of requests for sexual images of minors online. *Crime Science, 5*(1), 2. doi:10.1186/s40163-016-0050-0

Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime Science, 7*(5).

Rodríguez, J. I., Durán, S. R., Díaz-López, D., Pastor-Galindo, J., & Mármol, F. G. (2020). C3-Sex: A conversational agent to detect online sex offenders. *Electronics, 9*(11), 1779. doi:10.3390/electronics9111779

Röösli, M. (2022). *Actualité de TIP*. Paper presented at the SPIK 2022, Berne. https://www.swisspoliceict.ch/getattachment/SPIK/SPIK-2022/Agenda-6-April-2022/Plenum/PTI-Schweiz/20220406_PTI_SPIK_Prasentation_fr.pdf.aspx

Salter, M., & Whitten, T. (2021). A comparative content analysis of pre-Internet and contemporary child sexual abuse material. *Deviant Behavior, 0*(0), 1-15. doi:10.1080/01639625.2021.1967707

Schuhmann, P. (2020). *Zusammenhänge zwischen sexuellen Übergriffen auf Kinder und Konsum von Kindesmissbrauchsabbildungen bei Offline- und Online-Tätern.* (phdthesis), Universität Regensburg,

Schwegler, C. (2022a). Le réseau dans la lutte contre la cybercriminalité. Que fait NEDIK ?

Schwegler, C. (2022b). Poursuite pénale dans le domaine de la cybercriminalité au niveau fédéral. Du point de vue d'une procureure fédérale.

Seymour-Smith, S., & Kloess, J. A. (2021). A discursive analysis of compliance, resistance and escalation to threats in sexually exploitative interactions between offenders and male children. *British Journal of Social Psychology, 60*(3), 988-1011. doi:10.1111/bjso.12437

Sheehan, V. (2016). *Producers of indecent images of children : A qualitative analysis of the aetiology and development of their offending patterns.* (phdthesis), London Metropolitan University, repository.londonmet.ac.uk database.

Shelton, J., Eakin, J., Hoffer, T., Muirhead, Y., & Owens, J. (2016). Online child sexual exploitation: An investigative analysis of offender characteristics and offending behavior. *Aggression and Violent Behavior, 30*, 15-23. doi:10.1016/j.avb.2016.07.002

Soldino, V., Carbonell-Vayá, E. J., & Seigfried-Spellar, K. C. (2019). Criminological differences between child pornography offenders arrested in Spain. *Child Abuse & Neglect, 98*, 104178. doi:10.1016/j.chiabu.2019.104178

Soldino, V., Carbonell-Vayá, E. J., & Seigfried-Spellar, K. C. (2021). Spanish validation of the child pornography offender risk tool. *Sexual Abuse, 33*(5), 503-528. doi:10.1177/1079063220928958

Soldino, V., Merdian, H. L., Bartels, R. M., & Bradshaw, H. K. (2020). Implicit theories of child sexual exploitation material offenders: Cross-cultural validation of interview findings. *International Journal of Offender Therapy and Comparative Criminology, 64*(4), 315-334. doi:10.1177/0306624X19877599

Steel, C. M. S., Newman, E., O'Rourke, S., & Quayle, E. (2021). Collecting and viewing behaviors of child sexual exploitation material offenders. *Child Abuse & Neglect, 118*, 105133. doi:10.1016/j.chiabu.2021.105133

Steel, C. M. S., Newman, E., O'Rourke, S., & Quayle, E. (2020). An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders. *Forensic Science International: Digital Investigation, 33*, 300971. doi:10.1016/j.fsidi.2020.300971

Steely, M., Ten Bensel, T., Bratton, T., & Lytle, R. (2018). All part of the process? A qualitative examination of change in online child pornography behaviors. *Criminal Justice Studies, 31*(3), 279-296. doi:10.1080/1478601X.2018.1492389

Taylor, H. (2017). *Online sexual grooming: the role of offender motivation and grooming strategies.* (phdthesis), University of Birmingham, etheses.bham.ac.uk database.

van Dijk, J. J. M., & de Waard, J. (1991). A two-dimensional typology of crime prevention projects : With a bibliography. *Criminal justice abstracts*, 483-503.

van Gijn-Grosvenor, E. L., & Lamb, M. E. (2016). Behavioural differences between online sexual groomers approaching boys and girls. *Journal of Child Sexual Abuse, 25*(5), 577-596. doi:10.1080/10538712.2016.1189473

Ventéjoux, A. (2019). *Une lecture de la cyberviolence : la rencontre du sujet et du cyberespace dans les infractions à caractère sexuel envers mineurs réalisées sur Internet.* (phdthesis), Université Rennes 2, tel.archives-ouvertes.fr database.

Waller, G., Süss, D., Suter, L., Willemse, I., Külling, C., Bernath, J., Skirgaila, P., & Löpfe, S. (2021). *JAMESfocus – Retour sur une décennie d'études sur la jeunesse et les médias*. Université des sciences appliquées de Zurich. Zurich

Weingraber, S., Plath, C., Naegele, L., & Stein, M. (2020). Online victimization – an explorative study of sexual violence and cyber grooming in the context of social media use by young adults in Germany. *Social Work & Society, 18*(3).

Winters, G. M., Kaylor, L. E., & Jeglic, E. L. (2017). Sexual offenders contacting children online: an examination of transcripts of sexual grooming. *Journal of Sexual Aggression, 23*(1), 62-76. doi:10.1080/13552600.2016.1271146

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. J. J. o. A. H. (2018). Sextortion of minors: Characteristics and dynamics. *62*(1), 72-79.

Wolak, J., & Finklelhor, D. (2016). *Sextortion: Findings from a survey of 1,631 victims*. Crimes Against Children Research Center

Zermatten, A. (2017). Art. 187 CP. In A. Macaluso, L. Moreillon, & N. Queloz (Eds.), *Commentaire romand Code pénal II art. 111-392 CP*: Helbing Lichtenhahn.

Zöchbauer, B. (2021). *Cybergrooming im Pielachtal.* Fachhochschule FH Campus Wien

9. Annexes

Annexe A – Statistiques policières de la criminalité : les cyber-délits enregistrés en 2020

Tab. I : Caractéristiques des personnes lésées par un cyber-délit sexuel enregistré par la police en 2020

	Total victimes	**Tranches d'âge**							**Sexe**	
		<10	10-15	15-17	18-19	20-25	25+	s.n.	Masculin	Féminin
Cyber-délits sexuels	283	22	133	65	11	9	42	1	58	225
Pornographie interdite	145	16	68	36	3	3	18	1	32	113
Grooming	55	2	40	11	1	0	1	0	14	41
Sextorsion	78	2	20	20	7	6	23	0	11	67
Live-streaming	9	2	6	1	0	0	0	0	3	6

Source: Office fédéral de la statistique OFS, Tableau 19.02.09.01.03, Criminalité numérique : Mode opératoires de criminalité numérique et lésés, Suisse, Année 2020.

Tab. II : Caractéristiques des personnes prévenues pour un cyber-délit sexuel enregistré par la police en 2020

	Total prévenues	**Tranches d'âge**								**Sexe**	
		<18	18-19	20-24	25-34	35-49	50-69	70+	s.n.	Masculin	Féminin
Cyber-délits sexuels	1956	689	132	208	331	366	209	19	2	1748	208
Pornographie interdite	1848	651	125	198	312	346	196	19	1	1644	204
Grooming	73	22	3	9	16	11	12	0	0	70	3
Sextorsion	31	19	2	5	3	2	0	0	0	30	1
Live-streaming	20	2	3	0	1	10	3	0	1	20	0

Source : Office fédéral de la statistique OFS, Tableau 19.02.09.01.02, Criminalité numérique : Mode opératoires de criminalité numérique et personnes prévenues, Suisse, Année 2020.

Annexe B – Paramètres de recherche appliqués pour la revue de littérature

Paramètres de recherche suivis lors des revues de littérature sur les phénomènes

Moteur de recherche	Google Scholar
Période d'intérêt	Depuis 2016 (inclus)
Langues	Anglais, français et allemand
Mots clés	
Production et distribution de matériel pédopornographique via Internet[286]	(pornographie OR pédopornographie) AND (enfant* OR jeun* OR adolescent* OR mineur*) AND (production OR distribution) AND (auteur* OR victim* OR "modus operandi" OR "mode opératoire") (pornographie OR "misshandlung Material" OR "missbrauch Material") AND (kind* OR jung* OR minderjährig*) AND (Verteilung OR Produktion) AND (*Täter* OR Opfer* OR "Modus Operandi") (pornography OR "exploitation material" OR "sexual abuse material") AND (child* OR youth* OR juvenil* OR minor*) AND (production OR distribution) AND (offender* OR victim* OR "modus operandi")
Cyber grooming[287]	Cyber*grooming AND (auteur* OR victim* OR "modus operandi" OR "mode opératoire") Cyber*grooming AND (*Täter* OR Opfer* OR "Modus Operandi") Cyber*grooming AND (offender* OR victim* OR "modus operandi")
Sextorsion[288]	Sextortion AND (enfant* OR jeun* OR adolescent* OR mineur*) AND (auteur* OR victim* OR "modus operandi" OR "mode opératoire") Sextortion AND (kind* OR jung* OR minderjährig*) AND (*Täter* OR Opfer* OR "modus operandi") Sextortion AND (child* OR youth* OR juvenil* OR minor*) AND (offender* OR victim* OR "modus operandi")
Live-streaming[289]	Streaming AND sex* AND (enfant* OR jeun* OR adolescent* OR mineur*) AND (auteur* OR victim* OR "modus operandi" OR "mode opératoire") Live streaming AND sex* AND (kind* OR jung* OR minderjährig*) AND (*Täter* OR Opfer* OR "modus operandi") Live-streaming AND sex* AND (child* OR youth* OR juvenil* OR minor*) AND (offender* OR victim* OR "modus operandi")
Nombre de résultats	100 premiers résultats
Critères d'inclusion	a) avoir un titre ou un résumé pertinent ; b) traiter des caractéristiques des auteurs, des victimes ou du mode opératoire ; c) provenir d'Europe, d'Amérique du Nord et d'Australie

[286] Étant donné que ce phénomène a été extensivement étudié par la communauté académique, plusieurs termes ou expressions ont été choisis afin de représenter au mieux les diverses formulations utilisées pour nommer ce phénomène.
[287] Les résultats de la recherche exploratoire ont montré qu'il n'était pas nécessaire d'ajouter des termes ou expressions pour affiner les résultats de recherche sur Google Scholar.
[288] L'ajout des mots enfant, jeune et mineur a été nécessaire afin de cibler des publications ayant pour sujet la pratique de la sextorsion sur la population d'intérêt. Les recherches exploratoires ont montré que sans ces termes, les résultats n'étaient pas assez ciblés sur la thématique d'intérêt de ce projet.
[289] Étant une forme spécifique de production et de distribution de matériel sur Internet, l'ajout de termes ou d'expressions a été nécessaire afin d'obtenir des résultats en lien avec la thématique d'intérêt de ce projet. De plus, les résultats de la recherche exploratoire ont montré que sans cet ajout, les résultats obtenus dans Google Scholar n'étaient pas pertinents.

Variables et modalités répertoriées pour les manuscrits détectés

Titre de l'article	Titre de l'article
Auteur(s)	Nom de l'auteur avec l'année de publication
Zone géographique	Nom du pays où l'étude a été menée
Méthodologie	Méthodologie utilisée pour mener la recherche ainsi que la source de données et la méthode d'analyse
Période	Période temporelle investiguée dans le cadre de la recherche
Résultats	Description des principaux résultats obtenus, de manière la plus synthétique et détaillée possible

Annexe C – Échelle de COPINE, une typologie des images de pédopornographie

Level	Name	Description of Picture Qualities
1	Indicative	Non-erotic and non-sexualised pictures showing children in their underwear, swimming costumes, etc. from either commercial sources or family albums; pictures of children playing in normal settings, in which the context or organisation of pictures by the collector indicates inappropriateness
2	Nudist	Pictures of naked or semi-naked children in appropriate nudist settings, and from legitimate sources
3	Erotica	Surreptitiously taken photographs of children in play areas or other safe environments showing either underwear or varying degrees of nakedness
4	Posing	Deliberately posed pictures of children fully, partially clothed or naked (where the amount, context and organisation suggests sexual interest)
5	Erotic posing	Deliberately posed pictures of fully, partially clothed or naked children in sexualised or provocative poses
6	Explicit erotic posing	Deliberately posed pictures of fully, partially clothed or naked children in sexualised or provocative poses
7	Explicit sexual activity	Involves touching, mutual and selfsexual activity masturbation, oral sex and intercourse by child, not involving an adult
8	Assault	Pictures of children being subjected to a sexual assault, involving digital touching, involving an adult
9	Gross assault	Grossly obscene pictures of sexual assault, involving penetrative sex, masturbation or oral sex involving an adult
10	Sadistic / bestiality	a. Pictures showing a child being tied, bound, bestiality beaten, whipped or otherwise subjected to something that implies pain b. Pictures where an animal is involved in some form of sexual behaviour with a child

Note. Repris de Taylor et al., 2001.

Annexe D – Questionnaire en français adressé aux organisations potentiellement actives dans la mise en œuvre de mesures de protection

Variables et modalités répertoriées pour les mesures qui ont été reportées via le questionnaire

Le type d'organisation	Établissements scolaires / Police / Tribunaux des mineurs / Tribunaux pénaux de première instance / Départements gouvernementaux / Organisations de la société civile / Institut de médecine sociale et préventive / Organisations privées
Canton d'appartenance	Nom du Canton
Type de mesure selon le groupe cible et le type de prévention	Prévention vers le public (A1 auteurs / B1 victimes / C1 situations) Prévention vers les groupes à risque/situation (A2 auteurs / B2 victimes / C2 situations) Prévention vers les groupes principaux/situations (A3 auteurs / B3 victimes / C3 situations)
Cibles	Jeunes (tranches d'âge de l'enfance à l'adolescence) / Parents ou tuteurs / Enseignants / Professionnels : terme regroupant différents corps de métiers ayant un contact plus ou moins étroit avec des enfants ou des adolescents, qu'il s'agisse d'assistants sociaux, d'entraîneurs sportifs ou de policiers / Décideurs politiques / Auteurs : lorsque la mesure de prévention vise uniquement des (potentiels) auteurs d'infractions en ligne contre l'intégrité sexuelle de mineurs, peu importe leur tranche d'âge ou leur occupation / Public
Activités établies par les mesures	Formation (ex. intervention en classe, atelier) / Informations et conseils / Activité ludique et éducative / Aide et soutien (avec ou sans option de traitement) / Logiciel de contrôle et blocage / Plateforme de signalement / Charte de sécurité / Campagne de sensibilisation / Groupe de travail
Phénomène	Le cyber grooming La sextorsion La pédopornographie Le live-streaming de contenu à caractère pédopornographique Utilisation des médias en général, peu spécialisé

Acteurs et mesures de protection des enfants et des jeunes face aux cyber-délits sexuels

Dans le cadre de ce mandat, l'OFAS a identifié quatre formes en particulier de comportements répréhensibles. Il s'agit de cyber-délits sexuels qui impliquent l'entrée en contact d'une personne adulte avec un mineur à des fins sexuelles, mais sans qu'il n'y ait de rencontre « physique » : l'établissement du lien de confiance et les échanges se déroulent exclusivement en ligne.

• **Production et distribution de pédopornographie via Internet :** la pédopornographie comprend notamment les représentations de contenus sexuels, focalisées sur les organes sexuels d'un enfant et ayant pour but de susciter une excitation sexuelle.

• **(Cyber)grooming :** le fait, pour un adulte, d'établir des contacts avec des enfants via Internet à des fins sexuelles, par exemple dans des tchats ou sur les réseaux sociaux.

• **Sextortion :** contrainte ou forme de chantage exercée au moyen de matériel à caractère sexuel. Une personne se procure des photos osées d'une autre personne (mineure) via les réseaux sociaux ou des tchats. Elle menace ensuite de rendre ces images publiques afin d'obtenir davantage d'images ou d'argent de sa victime ou une rencontre.

• **Live-streaming d'actes d'ordre sexuel :** participation à des actes d'ordre sexuel avec des enfants via Webcam. Le criminel convainc ou oblige sa jeune victime à effectuer des actes d'ordre sexuel devant une caméra allumée ou paie une tierce personne pour abuser sexuellement de la victime selon ses instructions concrètes et pour diffuser en direct cet acte.

Merci de remplir les champs suivants :

Le nom de la personne de contact et son adresse email seront uniquement utilisés pour vous contacter si nous avons besoin d'informations complémentaires.

Nom de votre institution : _____

Personne de contact : _____

Email : _____

1. **Votre institution a-t-elle déjà développé ou participé à des initiatives en lien avec la protection des enfants et des jeunes face aux cyber-délits sexuels ?**

   Par initiative, nous entendons toute intervention ciblée et sélective visant à contrer le phénomène de cyber-délits sexuels contre les enfants et les jeunes (ex. campagne d'information, brochure informative, module de formation, filtres techniques, création d'un groupe de travail, convention sectorielle/partenariat, etc.)

   - □ Oui, notre institution a déjà développé des initiatives (⇨ passez directement à la question 2)
   - □ Oui, notre institution a déjà participé à des initiatives (⇨ passez directement à la question 2)
   - □ Non (⇨ passez directement à la question 9)

2. **Veuillez indiquer le nombre d'initiative que votre institution a développé ou auxquelles votre institution a participé :**

   [*Menu déroulant*]

   - □ 1
   - □ 2
   - □ 3
   - □ 4 – 9
   - □ 10 ou plus

   [*si plus de 3 à la question 2*] **Vous avez mentionné que votre institution a développé ou participé à plusieurs initiatives, merci de considérer les trois initiatives les plus importantes pour les prochaines questions.**

3. **Pouvez-vous nous décrire brièvement l'Initiative 1 ?**
   Notamment, nous vous prions d'indiquer le type d'activité, les acteurs impliqués, la portée de l'initiative (locale, cantonale, nationale), et la période temporelle.
   S'il existe une page web portant sur cette initiative, veuillez l'indiquer dans la réponse.

   _____

   _____

4. **Quel était le rôle de votre institution dans cette Initiative 1 ?**

   □ Organisateur·trice / coordinateur·trice

   □ Participant·e

5. [*si 2 ou plus à la question 2*] **Pouvez-vous nous décrire brièvement l'Initiative 2 ?**
   Notamment, nous vous prions d'indiquer le type d'activité, les acteurs impliqués, la portée de l'initiative (locale, cantonale, nationale), et la période temporelle.
   S'il existe une page web portant sur cette initiative, veuillez l'indiquer dans la réponse.

   _____

   _____

6. **Quel était le rôle de votre institution dans cette Initiative 2 ?**

   □ Organisateur·trice / coordinateur·trice

   □ Participant·e

7. [*si 3 ou plus à la question 2*] **Pouvez-vous nous décrire brièvement l'Initiative 3 ?**
   Notamment, nous vous prions d'indiquer le type d'activité, les acteurs impliqués, la portée de l'initiative (locale, cantonale, nationale), et la période temporelle.

   S'il existe une page web portant sur cette initiative, veuillez l'indiquer dans la réponse.

   _____

   _____

8. **Quel était le rôle de votre institution dans cette Initiative 3 ?**

   □ Organisateur·trice / coordinateur·trice

   □ Participant·e

9. **Votre institution fait-elle partie d'un réseau/groupe qui échange et discute de cette thématique ?**

   □ Oui (⇨ passez directement à la question 10)

   □ Non (⇨ passez directement à la question 14)

10. **Veuillez indiquer le nombre de réseaux auxquels votre institution est associée :**

    [*Menu déroulant*]

    □ 1

    □ 2

    □ 3

    □ 4 – 9

    □ 10 ou plus

    [*si plus de 3 à la question 10*] **Vous avez mentionné que votre institution est associée à plusieurs réseaux, merci de considérer les trois réseaux les plus importants pour les prochaines questions.**

11. Pouvez-vous nous décrire brièvement ce Réseau ?

Nous vous prions d'indiquer, si possible, le nom du réseau, ses activités et ses participant.e.s.

S'il existe une page web portant sur ce réseau, veuillez l'indiquer dans la réponse

_____

_____

12. [*si 2 ou plus à la question 10*] **Pouvez-vous nous décrire brièvement ce Réseau 2 ?**

Nous vous prions d'indiquer, si possible, le nom du réseau, ses activités et ses participant.e.s.

S'il existe une page web portant sur ce réseau, veuillez l'indiquer dans la réponse

_____

_____

13. [*si 3 ou plus à la question 10*] **Pouvez-vous nous décrire brièvement ce Réseau 3 ?**

Nous vous prions d'indiquer, si possible, le nom du réseau, ses activités et ses participant.e.s.

S'il existe une page web portant sur ce réseau, veuillez l'indiquer dans la réponse

_____

_____

14. Votre institution entretient-elle d'autres collaborations avec des organismes publics ou privés ou de professionnels pour discuter ou développer ces initiatives ?

- □ Oui (⇨ passez directement à la question 15)
- □ Non (⇨ passez directement à la question 16)

15. Pouvez-vous nous décrire brièvement ces collaborations, ses activités et ses participant.e.s ?

_____

_____

16. Si vous avez du matériel concernant les initiatives mises en place par votre institution (texte d'introduction, dépliants) et que vous jugez intéressant pour en savoir plus sur votre activité, n'hésitez pas à joindre les fichiers ci-dessous ou à nous les transmettre à l'adresse suivante : christine.burkhardt@unil.ch

[*champs upload*]

17a. [*si répondu Oui à la question 1*] **Votre institution a-t-elle prévu de développer ou participer, dans les prochains mois, à de nouvelles initiatives en lien avec la protection des enfants et des jeunes face aux cyber-délits sexuels ?**

- □ Oui (⇨ passez directement à la question 18)
- □ Non (⇨ passez directement à la question 19)

17b. [*si répondu Non à la question 1*] **Votre institution a-t-elle prévu de développer ou participer, dans les prochains mois, à des initiatives en lien avec la protection des enfants et des jeunes face aux cyber-délits sexuels ?**

- □ Oui (⇨ passez directement à la question 18)
- □ Non (⇨ passez directement à la question 19)

18. Pouvez-vous nous décrire brièvement cette ou ces initiative(s) ?

_____

_____

19. Avez-vous d'autres éléments à mentionner en lien avec la protection des enfants et des jeunes face aux cyber-délits sexuels ?

_____

_____

Le questionnaire est terminé, pour l'envoyer cliquez sur le bouton ENVOYER.

Nous vous remercions infiniment pour votre collaboration !

Annexe E – Grilles d'entretien

Liste de questions pour les experts suisses

A. Introduction - Questions générales

1. Questions biographiques sur la personne interviewée (éducation, années d'expérience sur le terrain, responsabilités, recherches et travaux sur le terrain en général).
2. Pouvez-vous nous décrire brièvement votre expérience en matière de mesures de protection des enfants et des jeunes face aux cyber-délits sexuels.
3. Par rapport à la liste de mesures en Suisse que vous avez reçue, y a-t-il d'autres mesures actives qui n'ont pas été mentionnées ?

B. Cyber-délits sexuels sur les enfants et les jeunes en Suisse : avis général sur le phénomène et sur les mesures existantes

4. Comment comprenez-vous les phénomènes de cyber-délits sexuels sur les enfants et les jeunes en Europe, quelles sont les principales caractéristiques, et quels sont les problèmes/challenges les plus urgents dans ce domaine (aussi par rapport à d'autres zones géographiques) ?

   Sous-questions : Quelles sont les activités et les plateformes les plus à risque sur Internet ? Quelles sont les caractéristiques principales des victimes et des agresseurs ?

5. Comment considérez-vous l'ensemble de mesures de protection de cyber-délits sexuels sur les enfants et les jeunes, quel est votre opinion sur leur implémentation en Europe, et quels sont les actions les plus urgentes à prendre dans ce domaine ?

C. Questions spécifiques sur les mesures, efficaces, prometteuses, plutôt inefficaces

6. Au niveau de la [prévention sociale – prévention situationnelle - police et coopération policière – justice et réglementation]*, parmi les mesures recensées en Suisse, pouvez-vous nous indiquer celles qui vous semblent les plus efficaces/prometteuses aujourd'hui ? Pouvez-vous nous donnez une explication à sujet.
   ** A adapter en fonction du profil de l'expert.*
7. Pouvez-vous nous indiquer quelles mesures vous semblent les moins efficaces ? Pouvez-vous nous donnez une explication à ce sujet.
8. Pouvez-vous nous indiquer les principales innovations qui devraient être implémentées en Suisse dans les différents domaines ?

D. Conclusion

9. Nous arrivons à la fin de l'entretien, j'ai une dernière question : connaissez-vous un expert dans le domaine ou une organisation qu'il serait pertinent d'interviewer pour notre étude ?
10. Avant de terminer l'entretien, souhaiteriez-vous ajouter quelque chose ?

Questions additionnelles dans la limite du temps imparti

- Sur la base de votre expérience, quel a été l'impact de la pandémie sur les cyber-délits sexuels contre les enfants et les jeunes ?
- Dans ce contexte, quelles mesures urgentes devraient être prises pour protéger les enfants et les jeunes ?

Liste de questions pour les experts d'autres pays

A. Introduction - Questions générales

1. Questions biographiques sur la personne interviewée (éducation, années d'expérience sur le terrain, responsabilités, recherches et travaux sur le terrain en général).
2. Pouvez-vous nous décrire brièvement votre expérience en matière de mesures de protection des enfants et des jeunes face aux cyber-délits sexuels.

2. Cyber-délits sexuels sur les enfants et les jeunes en Suisse : avis général sur le phénomène et sur les mesures existantes

3. Comment comprenez-vous les phénomènes de cyber-délits sexuels sur les enfants et les jeunes en Europe, quelles sont les principales caractéristiques, et quels sont les problèmes/challenges les plus urgents dans ce domaine (aussi par rapport à d'autres zones géographiques) ?

   Sous-questions : Quelles sont les activités et les plateformes les plus à risque sur Internet ? Quelles sont les caractéristiques principales des victimes et des agresseurs ?

4. Comment considérez-vous l'ensemble de mesures de protection de cyber-délits sexuels sur les enfants et les jeunes, quel est votre opinion sur leur implémentation en Europe, et quels sont les actions les plus urgentes à prendre dans ce domaine ?

3. Questions spécifiques sur les mesures, efficaces, prometteuses, plutôt inefficaces

5. Au niveau de la [prévention sociale – prévention situationnelle - police et coopération policière – justice et réglementation]*, parmi les mesures recensées en Suisse, pouvez-vous nous indiquer celles qui vous semblent les plus efficaces/prometteuses aujourd'hui ? Pouvez-vous nous donnez une explication à sujet.

   ** A adapter en fonction du profil de l'expert.*

6. Pouvez-vous nous indiquer quelles mesures vous semblent les moins efficaces ? Pouvez-vous nous donnez une explication à ce sujet.
7. Pouvez-vous nous indiquer les principales innovations qui devraient être implémentées en Suisse dans les différents domaines ?

D. Conclusion

8. Nous arrivons à la fin de l'entretien, j'ai une dernière question : connaissez-vous un expert dans le domaine ou une organisation qu'il serait pertinent d'interviewer pour notre étude ?
9. Avant de terminer l'entretien, souhaiteriez-vous ajouter quelque chose ?

Questions additionnelles dans la limite du temps imparti

- Sur la base de votre expérience, quel a été l'impact de la pandémie sur les cyber-délits sexuels contre les enfants et les jeunes ?
- Dans ce contexte, quelles mesures urgentes devraient être prises pour protéger les enfants et les jeunes ?

Annexe F – Formulaire d'information et de consentement

UNIL | Université de Lausanne
Faculté de droit, des sciences criminelles
et d'administration publique

FORMULAIRE D'INFORMATION ET DE CONSENTEMENT

INFORMATION SUR L'ETUDE

Titre de l'étude

Mesures de protection des enfants et des jeunes face aux cyber-délits sexuels – Etude mandatée par l'Office fédérale des assurances sociales (OFAS) 164000650

Equipe de recherche

Responsable du projet

Dr Stefano Caneppele
Professeur
Ecole des sciences criminelles, Université de Lausanne
stefano.caneppele@unil.ch

Co-chercheur·e·s

Christine Burkhardt
Chargée de recherche
Ecole des sciences criminelles, Université de Lausanne
christine.burkhardt@unil.ch

Fabian Muhly
Chargé de recherche
Ecole des sciences criminelles, Université de Lausanne
fabian.muhly@unil.ch

Objet de l'étude

La présente étude – mandaté par l'Office fédéral des assurances sociales (OFAS) – vise à donner un aperçu des mesures de protection des enfants et des jeunes contre les cyber-délits sexuels, et des actrices et acteurs actifs dans le domaine de la prévention et de la répression en Suisse. Il s'agit de relever quelles sont les pratiques prometteuses qui existent et quelles sont les possibilités d'amélioration et les limites des différentes mesures mises en place en Suisse et en Europe. Sur cette base, il sera possible de formuler des recommandations pour la Suisse.

UNIL | Université de Lausanne
Faculté de droit, des sciences criminelles
et d'administration publique

Dans une première phase, les chercheur·e·s ont identifié les mesures de protection mises en place en Suisse, ainsi que les acteurs institutionnels actifs dans le domaine. Une deuxième phase consiste à mener des entretiens avec des experts, suisses et européens, afin de recueillir leurs opinions sur l'efficacité, les limitations et les possibilités d'amélioration des mesures actuellement implémentées en Suisse et en Europe.

Votre participation à notre étude s'inscrit dans cette seconde phase.

Participation à l'étude

Votre participation consiste à prendre part à un entretien individuel, en visioconférence (Zoom ou MS Teams), d'une durée d'environ une heure. Au cours de cet entretien, nous vous demanderons votre avis sur les phénomènes de cyber-délits sexuels sur les enfants et les jeunes, les mesures de protection mises en place et leur efficacité, ainsi que les améliorations et les innovations attendues pour le futur.

Confidentialité et traitement des données

L'entretien sera enregistré directement via la plateforme de visioconférence utilisée (Zoom ou MS Teams). Le fichier audio sera stocké en toute sécurité sur des dispositifs protégés par un mot de passe. Le fichier audio sera définitivement détruit après retranscription de l'entretien, ou au plus tard en août 2022.

Les informations récoltées lors de l'entretien seront utilisées uniquement pour rédiger le rapport dans le cadre du présent mandat, ainsi qu'un article qui paraitra dans la revue électronique de l'OFAS *Sécurité sociale CHSS*.

Participation volontaire et droit de retrait

Votre participation est entièrement volontaire et sans compensation. Vous êtes libre de vous retirer en tout temps, sans avoir à justifier votre décision. Le cas échéant, les renseignements personnels vous concernant seront détruits.

UNIL | Université de Lausanne
Faculté de droit, des sciences criminelles
et d'administration publique

CONSENTEMENT

Je déclare avoir pris connaissance des informations ci-dessus, avoir obtenu les réponses à mes questions sur ma participation à l'étude et comprendre le but et la nature de cette étude.

Si vous consentez à participer à cette étude, merci de bien vouloir cocher les deux cases :

☐ Ma participation est volontaire et je n'ai pas été contraint à répondre à cet entretien.

☐ J'accepte que mes réponses à cet entretien soient utilisées par l'équipe de recherche pour la rédaction du rapport adressé à l'Office fédéral des assurances sociales (OFAS) et pour un article qui paraitra dans la revue électronique de l'OFAS *Sécurité sociale CHSS*.

Merci de bien vouloir cocher la case ou les cases qui conviennent
En tant que participant·e à cette étude

☐ J'accepte d'être identifié·e par mon nom, ma fonction et mon affiliation.

☐ Je ne souhaite pas être identifié·e par mon nom, mais j'accepte d'être cité·e par ma fonction.

☐ Je ne souhaite pas être identifié·e par mon nom, mais j'accepte d'être cité·e par mon affiliation.

☐ Je ne souhaite pas être identifié·e par mon nom, ma fonction ou mon affiliation.

Nom, Prénom :
Affiliation :
Signature :
Date :
Fonction :

Pour toute question relative à cette étude, vous pouvez communiquer avec Madame Christine Burkhardt, à l'adresse courriel suivante **christine.burkhardt@unil.ch**

Annexe G – Paramètres de recherche appliqués pour la recension des mesures

Paramètres de recherche suivis pour détecter les mesures de protection sur le moteur de recherche en ligne

Production et distribution de matériel pédopornographique via Internet	(measure OR initiative OR campaign) AND (prevention OR protection) AND (child abuse material OR child pornography) (pornography OR "exploitation material" OR "sexual abuse material") AND (child* OR youth* OR juvenil* OR minor*) AND (measure OR initiative OR campaign) (mesure OR initiative OR campagne) AND (prévention OR protection) AND (pédopornographie OU pornographie infantile) (pornographie OR pédopornographie) AND (enfant* OR jeune* OR adolescent* OR mineur*) AND (mesure OR initiative OR campagne) (Mittel OR Initiative OR Kampagne) AND (Prävention OR Schutz) AND Kinderpornografie (pornographie OR "misshandlung Material" OR "missbrauch Material") AND (kind* OR jung* OR minderjährig*) AND (Massnahmen OR Initiative OR Kampagne) (misura OR iniziative OR campagna) AND (prevenzione OR protezione) AND (pornografia infantile OR pedopornografia) (pornografia OR pedopornografia) AND (bambin* OR giovan* OR adolescent* OR minor*) AND (misura OR iniziativa OR campagna)
Cyber grooming	(measure OR initiative OR campaign) AND (prevention OR protection) AND grooming cyber*grooming AND (measure OR initiative OR campaign) (mesure OR initiative OR campagne) AND (prévention OR protection) AND grooming cyber*grooming AND (mesure OR initiative OR campagne) (Mittel OR Initiative OR Kampagne) AND (Prävention OR Schutz) AND grooming cyber*grooming AND (Massnahmen OR Initiative OR Kampagne) (misura OR iniziative OR campagna) AND (prevenzione OR protezione) AND grooming cyber*grooming AND (misura OR iniziativa OR campagna)
Sextorsion	(measure OR initiative OR campaign) AND (prevention OR protection) AND sextortion sextortion AND (measure OR initiative OR campaign) (mesure OR initiative OR campagne) AND (prévention OR protection) AND sextortion sextortion AND (mesure OR initiative OR campagne) (Mittel OR Initiative OR Kampagne) AND (Prävention OR Schutz) AND sextortion sextortion AND (Massnahmen OR Initiative OR Kampagne) (misura OR iniziative OR campagna) AND (prevenzione OR protezione) AND sextortion sextortion AND (misura OR iniziativa OR campagna)
Live-streaming de pédopornographie	(measure OR initiative OR campaign) AND (prevention OR protection) AND live streaming live-streaming AND sex* AND (child* OR youth* OR juvenil* OR minor*) AND (measure OR initiative OR campaign) (mesure OR initiative OR campagne) AND (prévention OR protection) AND (diffusion en direct OU streaming) (Streaming OR diffusion en direct) AND sex* AND (enfant* OR jeune* OR adolescent* OR mineur*) AND (mesure OR initiative OR campagne) (Mittel OR Initiative OR Kampagne) AND (Prävention OR Schutz) AND live-streaming Live streaming AND sex* AND (kind* OR jung* OR minderjährig*) AND (Massnahmen OR Initiative OR Kampagne) (misura OR iniziative OR campagna) AND (prevenzione OR protezione) AND live-streaming diretta streaming AND sex* AND (bambin* OR giovan* OR adolescent* OR minor*) AND (misura OR iniziativa OR campagna)

Weitere Forschungs- und Expertenberichte aus der Reihe «Beiträge zur Sozialen Sicherheit»

Autres rapports de recherche et expertises de la série «Aspects de la sécurité sociale»

Altri rapporti di ricerca e perizie della collana «Aspetti della sicurezza sociale»

Further research reports and expertises in the series «Beiträge zur Sozialen Sicherheit»