# La face obscure d'Internet

# Le matériel pédopornographique sur les Darknets

Rob Wainwright, directeur d'EUROPOL, a ouvert la "Conférence européenne 2015 sur la grande criminalité organisée", en constatant que tout pouvait être acheté et vendu impunément sur les « Darknets »[1]. Par conséquent, ces derniers sont une préoccupation croissante pour les forces de l'ordre car ils abritent des marchés illicites où les criminels professionnels (pirates informatiques, faussaires, marchands d'armes ou de drogues) peuvent offrir leurs services en toute impunité. Même si la majorité des utilisateurs des Darknets sont défavorables à la diffusion de matériel pédopornographique [2], le dénominateur commun de cet Internet souterrain est un rejet complet de toute censure. De ce fait, les marchés et les forums contenant du matériel pédopornographique trouvent ainsi un refuge sûr dans les Darknets et en composeraient même 80 % des flux selon une étude récente[3].

Cette analyse se focalisera donc sur la face cachée d'Internet en relation avec le matériel pédopornographique. Après avoir resitué le Darknet dans la réalité qui l'a vu naître, elle se penchera sur l'utilisation spécifique de l'Internet "obscur" dans le contexte de l'exploitation sexuelle commerciale des enfants ainsi que les obstacles rencontrés par les forces de l'ordre pour lutter contre ce phénomène.

## I. Qu'est-ce qu'un Darknet ?

[1] Littéralement "Internet obscur", les Darknets constituent une petite partie du Web invisible qui a été intentionnellement cachée. Ce sont des réseaux privés entre pairs (peer-to-peer ou P2P networks en anglais) garantissant l'anonymat à leurs utilisateurs, notamment pour l'échange de fichiers. Ils sont accessibles via un navigateur/logiciel spécifique. Tor et Freenet figurent parmi les Darknets les plus connus.

[2] Bien que, par commodité, ce terme soit communément utilisé dans les publications destinées au grand public, il est découragé au profit de « matériel relatif à la maltraitance sexuelle des enfants ». Cf. Rapport du Secrétaire des Nations Unies E/CN.15/2014/7, p.4. En effet, le terme "pédopornographie" pourrait laisser croire que c'est une des formes "acceptables" de pornographie, minimisant la violence sexuelle commise à l'encontre des enfants victimes.

[3] http://www.theguardian.com/technology/2014/dec/31/dark-web-traffic-child-abuse-sites.

En 2001, Michael K. Bergman utilisait la métaphore de l'océan pour décrire Internet : « Aujourd'hui, faire des recherches sur Internet peut être comparé à glisser un filet sur la surface de l'océan: une quantité importante d'informations peut être saisie mais il reste une foule de renseignements située en profondeur qui nous échappe »[4]. Quinze ans après et malgré le développement extrêmement rapide des nouvelles technologies, la formule de Bergman reste encore valable. Le Web invisible[5] et les Darknets ne sont pas perceptibles pour la plupart des utilisateurs d'Internet.

« Les Darknets utilisent l'infrastructure d'Internet mais restent à l'écart de celle-ci »[6] - c'est une des définitions les plus précises de cette réalité. Intégrés au grand réseau du Web invisible, les Darknets possèdent plusieurs caractéristiques communes qui les définissent : ils utilisent une technologie d'anonymat décentralisée, basée sur la structure d'Internet mais qui opère séparément du système classique et n'est pas accessible pour un utilisateur lamda[7]. Les réseaux les plus connus de Darknets sont Freenet, Tor, et I2P (« Invisible Internet Project »). Ce ne sont pas des réseaux homogènes mais bien de multiples groupes divisés par intérêt, langue et affinités. Quelle que soit l'activité, les Darknets offrent un refuge à leurs utilisateurs en leur garantissant l'anonymat.

Initialement crée en 2002 par le « US Naval Research Laboratory », le réseau Tor[8] est aujourd'hui géré par des volontaires et a largement dépassé son objectif premier. Accessible en configurant le pack de navigation Tor, il permet de naviguer et de poster des pages de manière complètement anonyme à l'intérieur du réseau. Le contenu pédopornographique y est abondant et classé selon les goûts des utilisateurs. On peut trouver des sous-catégories comme « hard candy» ou « jailbait ». Le premier terme est généralement utilisé comme synonyme du matériel pédopornographique impliquant des enfants pré-pubères, alors que « jailbait » est un mot d'argot désignant une jeune adolescente attirante.

---

[4] Bergman M.K. (2001). White Paper: *The Deep Web. Surfacing Hidden Value*, in «The Journal of Electronic Publishing», 7 (1), disponible sur: http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main.

[5] Le web invisible ou web caché désigne la partie du web qui n'est pas accessible directement aux moteurs de recherche traditionnels. Elle comprend l'ensemble des documents non indexés par les outils de recherche comme Google, Safari, Yahoo, etc. : les sources dont l'accès est contrôlé par un mot de passe, les sites possédant une base de données interne, les pages accessibles par un formulaire de recherche, les documents non référencés (volontairement ou non), les intranets, les extranets... (http://maboite.qc.ca/glossaire.php - w).

[6] Mansfield-Devine S. (2009), *Darknets*, «Computer Fraud & Security», 2009 (12), pp. 4-6.

[7] Ibidem

[8] https://www.torproject.org/

Freenet[9] est un autre Darknet populaire créé en 1999 par Ian Clarke. Bien que Freenet ait été créé en utilisant une technologie différente de Tor, le résultat final reste le même: garantir l'anonymat et contourner la censure d'Internet. Le matériel pédopornographique est ici mélangé à d'autres sortes de contenu : des blogs, des archives, des manifestes politiques et du contenu piraté. Freenet possède également sa propre application P2P - Frost, qui permet le partage simple et rapide de fichiers et la communication entre plusieurs utilisateurs en même temps. Frost se targue également de posséder des douzaines de services de messagerie instantanée dédiés à l'échange de matériel pédopornographique.

Les sites utilisés pour la distribution et l'échange de matériel pédopornographique vont des « image boards » (« forums à image ») aux forums de discussion. Le contenu peut être organisé de différentes manières : de la plus simple dissociation entre les filles et les garçons, à une organisation plus élaborée, par exemple selon le type de matériel pédopornographique (vidéos, photos, etc.), selon le producteur, la série d'images ou l'apparition d'un enfant en particulier. Les images sont publiées directement en pièces jointes à un message, tandis que les vidéos et les archives d'images sont le plus souvent téléchargées sur des sites d'hébergement de fichiers (cyberlockers). Le lien vers ce contenu accompagné du mot de passe est ensuite rendu public sur des forums de discussion ou par d'autres moyens, souvent accompagné de quelques « échantillons » (photos ou captures d'écran).

## II. Le matériel pédopornographique sur les Darknets: une tendance bien établie

L'opacité des Darknets est exactement ce qui attire les nombreuses activités illégales, parmi lesquelles figure la diffusion de matériel pédopornographique. L'échange de matériel pédopornographique se distance de plus en plus de la partie publique d'Internet, en suivant la devise « la sécurité par l'obscurité ». En effet, grâce aux efforts constants des ONG et des forces de l'ordre, la probabilité de tomber sur du matériel pédopornographique par hasard en surfant sur Internet devient de plus en plus réduite. Par conséquent, les délinquants sexuels se retranchent dans la partie moins visible du Net. Contrairement à ce que l'on

[9] https://freenetproject.org/

pourrait penser, le mode d'emploi des Darknets est assez facile à trouver et ce marché de pédopornographie est facilement accessible[10].

Les agences européennes de lutte contre le crime estiment qu'une part minime seulement, environ 7 à 10% du matériel pédopornographique en ligne, serait échangé à des fins commerciales[11]. Selon la Coalition Financière Européenne Contre l'Exploitation Sexuelle des Enfants à des fins commerciales sur Internet, un changement notable est en train de s'opérer, initié en premier lieu par les utilisateurs des Darknets. Auparavant, une distinction claire pouvait être faite entre l'échange de matériel pédopornographique à des fins commerciales, effectué par des individus motivés par le profit et n'ayant pas ou peu d'intérêt sexuel pour ces enfants, et l'échange de matériel à des fins non commerciales par des individus ayant une attirance sexuelle exclusive ou principale pour les enfants, mais ne recherchant que très rarement à tirer un profit financier de ces images.

Cette séparation traditionnelle est en train d'évoluer. En effet, au vu de la demande exponentielle pour des nouveaux matériels et donc de leur valeur commerciale intrinsèque, la deuxième catégorie d'individus est devenue de plus en plus entrepreneuriale en revendant plutôt qu'en échangeant ces nouvelles images [12]. Cette tendance est préoccupante car la demande de matériel pédopornographique ne faiblit pas. Au contraire, avec la démocratisation de l'accès à Internet dans le monde, elle pourrait augmenter dans les années à venir. Cela signifie que l'incitation à l'exploitation sexuelle des enfants afin de stimuler la production et la distribution de nouveaux matériels pédopornographiques pourrait augmenter.

Par ailleurs, malgré la série notoire d'opérations policières effectuées au sein du réseau, comme l'Opération Onymous [13], la popularité de Tor pour l'échange de matériel pédopornographique n'a pas semblé être ébranlée. Bien au contraire, avec une variété croissante de dispositifs conçus pour faciliter la connexion à ce Darknet, Tor continuera

[10] EUROPOL, « Virtual Global Taskforce Environmental Scan 2012 », p. 16, disponible sur: https://www.europol.europa.eu/content/virtual-global-taskforce-environmental-scan-2012
[11] Coalition Financière Européenne Contre l'Exploitation Sexuelle des Enfants à des fins commerciales sur Internet, « Strategic Assessment of Commercial Sexual Exploitation of Children Online », 2015, p. 5-6, disponible sur: http://www.europeanfinancialcoalition.eu/private10/images/news/pdf/65.pdf.
[12] Ibidem.
[13] http://www.janes.com/article/47455/law-enforcement-struggles-to-control-darknet.

d'être le réseau favori pour la distribution et le téléchargement de matériel pédopornographique.

## III. Les obstacles posés par les Darknets dans la lutte contre le matériel pédopornographique en ligne

Les services policiers nationaux, européens et internationaux font face à des obstacles récurrents afin de mettre un terme aux opérations illégales sur les Darknets. Ces obstacles sont dus aux technologies sur lesquelles les réseaux sont construits, et qui sont spécialement conçues pour protéger l'anonymat des utilisateurs. Les crypto-monnaies utilisées pour obtenir des matériels à caractère pédopornographique sur les Darknets sont également un problème majeur pour les forces de l'ordre: le *Bitcoin*[14] et ses équivalents, comme *Litecoin* ou *Zetacoin*, peuvent faire l'objet d'échanges successifs sans toutefois que l'on puisse en identifier le propriétaire initial[15]. La combinaison de ces deux facteurs à savoir un environnement anonyme sur les Darknets et l'utilisation de crypto-monnaies difficilement traçables fait que les utilisateurs opèrent dans un contexte relativement sécurisé.

L'autre défi important est le visionnage en direct d'abus sexuels commis sur des enfants (le live streaming child sexual abuse). Parce que commises en direct, ces infractions ne laissent que très peu de preuves, si elles ne sont pas localisées au moment même ou enregistrées. De nombreux pays ont reconnu la possession de matériel pédopornographique comme infraction pénale mais seulement quelques-uns ont aussi inclus l' « accès volontaire » dans sa définition. La différence de terminologie juridique est cruciale en cas d'abus sexuel filmé en direct (via skype par exemple) puisque le contenu n'est pas téléchargé par l'utilisateur: la personne y a accès volontairement - elle le visionne - mais elle ne le possède pas.

De plus, et toujours au niveau législatif, la victime et l'agresseur dépendent de juridictions différentes dans la majorité des cas. Par conséquent, le succès des enquêtes concernant le matériel pédopornographique dépendra largement de l'harmonisation des définitions

[14] Une crypto-monnaie est une monnaie électronique pair à pair et décentralisée dont la mise en oeuvre se base sur les principes de la cryptographie pour valider les transactions et la génération de la monnaie elle-même https://bitcoin.org/fr/
[15] http://www.janes.com/article/47455/law-enforcement-struggles-to-control-darknet.

légales, des procédures de coopération et de la communication entre les différentes autorités.

Le manque de preuves engendré par la production de matériel pédopornographique en direct est un obstacle majeur pour l'identification et la localisation des victimes afin de les protéger du milieu abusif dans lequel elles évoluent. Chaque nouveau contenu pédopornographique signifie qu'un nouvel enfant est victime d'abus sexuels. Les forces de l'ordre et les organisations non-gouvernementales (ONG) ont donc comme priorité d'identifier ces victimes à partir d'indices présents dans les matériels (un objet spécifique dans la pièce, une marque de vêtement, etc.). Or, cette analyse nécessite de se baser sur un enregistrement.

La seule vulnérabilité qui reste à exploiter par les autorités provient de l'erreur humaine : la plupart des arrestations sur des Darknets ont été possibles grâce à la négligence de quelques utilisateurs ayant révélé des informations personnelles[16] et non par les compétences technologiques des services répressifs.

## IV. Conclusion

Les utilisateurs de matériels pédopornographiques sont souvent très à la pointe au niveau technologique et utilisent les plateformes les plus sûres pour commettre leurs méfaits. Les Darknets – face cachée d'Internet et inconnue de la plupart des utilisateurs - représentent le dernier stade de cette évolution. Ils sont un défi permanent pour les forces de l'ordre: l'anonymisation, et les fonctions de cryptage des Darknets, ainsi que les crypto-monnaies utilisées pour payer ces contenus illégaux, l'absence de preuve en cas de retransmission en direct d'agression sexuelle et enfin, la nature internationale de cette infraction, freinent le processus d'identification des agresseurs et des victimes. Bien que ces technologies soient également utilisées pour des activités légales, la réticence à imposer tout type de censure dans ce milieu fournit un espace idéal pour la distribution de matériel pédopornographique.

[16] David Glance „Despite Darknet drug market arrests and seizures, can they be stopped?“: http://theconversation.com/despite-darknet-drug-market-arrests-and-seizures-can-they-be-stopped-33867 http://www.wired.com/2013/10/thompson/.

Alors que les outils répressifs traditionnels ne sont pas très efficaces en ce qui concerne les Darknets, de nouvelles solutions sont nécessaires pour lutter contre la diffusion de matériel pédopornographique. Une coopération plus étroite avec les ONG et tous les autres acteurs de première ligne est absolument nécessaire pour aborder le problème de manière plus créative, comme le démontre le cas « Sweetie »[17] ou le Photo DNA créé par Microsoft[18].

Cette analyse a été réalisée par Justė Neverauskaitė en juin 2015 sous la coordination d'ECPAT Belgique.

ECPAT Belgique est le membre belge officiellement reconnu du réseau ECPAT (End Child Prostitution, Child Pornography and Trafficking of Children for sexual purposes). La mission d'ECPAT Belgique est de lutter contre l'exploitation sexuelle des enfants à des fins commerciales. L'exploitation sexuelle commerciale des enfants recouvre différentes formes : la prostitution enfantine, la pornographie mettant en scène des enfants, la traite des enfants à des fins sexuelles et le tourisme sexuel impliquant des enfants.

**ECPAT Belgique**
**Rue du Marché aux Poulets, 30**
**1000 Bruxelles**
**Tél: 02/522.63.23**
**Email:** info@ecpat.be

[17] Voir l'analyse d'ECPAT Belgique "Matériel pédopornographique et Internet: Un défi permanent pour les forces de l'ordre", juin 2015, p. 2.
[18] L'empreinte numérique (Photo DNA ou Hash value) est un code unique attribué à une image afin de pouvoir la retrouver et identifier ses copies. http://www.zdnet.com/article/microsoft-joins-the-fight-against-child-pornography/