Le Dark Web : Une Perspective Positive

Samantha Schmidt, Ariadne Melissargos, Jérémy Martin, Michaël Desgalier

Etudiant-e-s en ingénierie des médias, 1ère année, HEIG-VD

Le *Dark Web*, sombre ou caché, s'assimile généralement à un espace clandestin. Du trafic de drogue, à la pornographie infantile, en passant par le vol de données, la vente d'armes et de contrefaçons, il n'a rien pour plaire. Pourtant, bon nombre de ses géniteurs n'étaient pas mal intentionnés. Pour la protection des données, il n'y a pas mieux. Le débat est vieux comme internet : surveiller pour sécuriser, interdire l'anonymat, jusqu'au pseudonymat sur les réseaux sociaux, même combat ! Et si nous apprenions à bien nous en servir ?

I. INTRODUCTION

Dans notre société moderne, la liberté de la presse fait face à de nombreux défis. Censure, diffamations, intimidations, poursuites judiciaires, emprisonnements et homicides touchent les journalistes du monde entier [1]. En partie initié afin de fournir un moyen sûr et sécurisé de communiquer et d'échanger des informations, le *Dark Web* possède un fort potentiel en tant que média pour la liberté de presse. Imbattable en termes d'anonymat, pour collaborer dans l'ombre et lancer des alertes, cette partie du Web où l'on ne va pas par hasard soulève des questions éthiques et juridiques apparemment insolubles.

II. UN DARKWEB ET DES DARKNETS

Le *Dark Web* fait partie du *Deep Web,* qui est ce qu'on appelle la partie « cachée » du Web.

Cet espace informationnel n'est pas accessible via les moteurs de recherche standards. D'une part, parce qu'il comprend des pages et des sites non indexés, d'autre part parce que les contenus qu'il abrite ne sont pas recensés dans un répertoire.

En effet, bien qu'il soit construit sur l'internet public, le *Dark Web* n'est accessible qu'avec des logiciels ou des protocoles qui lui sont spécifiques.

I2P (pour Invisible Internet Project) est un *darknet*, soit un réseau crypté qui fonctionne sans serveur, grâce aux connexions et aux échanges entre les ordinateurs des participants (*peer to peer* pour désigner les pairs). Les communications passent d'un utilisateur à un autre en empruntant des chemins détournés (en passant par d'autres utilisateurs). Plus il y a d'utilisateurs, plus le réseau est efficace, et plus il est difficile de retracer les chemins. En outre, le rôle d'expéditeur, de destinataire, et celui de relais de transmission sont parfaitement similaires. Un observateur ne peut donc pas affirmer que tel message était destiné à telle personne.

TOR (pour *The Onion Router*) est le *darknet* le plus connu. Il s'agit également d'un réseau « superposé », ou un réseau dans le réseau. À l'inverse d'I2P, il repose sur des serveurs dont la liste est publique, soit environ 7'000 relais dont l'objectif technique consiste à masquer l'adresse IP des visiteurs, celle-là même qui est tant convoitée par les analyseurs de trafic. Pour s'y rendre, il faut un navigateur Tor, qui permet de consulter les sites en « .onion », le nom de domaine (comme « .com » ou « .ch ») spécifique au réseau. De même, différents outils sont disponibles pour permettre à tout un chacun de publier ou d'héberger son propre contenu. Développé dans les années '90 par l'US Navy pour protéger les télécommunications, le projet reçoit en 2010 le prix du logiciel libre[1], dans la catégorie « projet d'intérêt social »[2] !

C'est donc le *darknet* qui héberge le *Dark Web*. I2P, Tor, Freenet, Zeronet… et bien d'autres encore, sont des initiatives qui mettent en œuvre des technologies différentes, pour poursuivre des objectifs similaires. En quelques mots : réserve, prudence, discrétion, secret, intimité, anonymat...

Dans les médias, le *Dark Web* est systématiquement associé à des activités illégales ou criminelles. Pourtant, il couvre de nombreuses utilisations légitimes telles que la lutte contre les régimes totalitaires ou la préservation des conversations privées.

III. CONTOURNER LA CENSURE ET LA SURVEILLANCE

Différents pays aux régimes stricts s'efforcent de contrôler l'opinion publique et les médias. Des contenus jugés tendancieux peuvent être rendus inaccessibles et la liberté d'expression n'est pas garantie.

Parce que certaines nations comme la Chine, l'Iran ou le Vietnam ont tenté de bloquer l'accès au site ou aux programmes de la BBC, la chaîne a rendu son site accessible via le réseau Tor en 2019. À ce jour, BBC News est accessible en russe ou en ukrainien via des adresses en « .onion ».[8]

Trois ans plus tôt, ProPublica, un média d'investigation, est connu pour être le premier à avoir lancé une version « sombre » de son site. Il propose ainsi un lien Tor qui promet aux utilisateurs un anonymat plus important, en accord avec ses thématiques principales ; la censure médiatique, la confidentialité et le tracking[2]. [3]

Depuis lors beaucoup d'autres ont suivi, à l'exemple du New York Times, du Guardian, de la Deutsche Welle, une radio allemande, ou même de Facebook.

Ainsi, le *Dark Web* offre un « autre » accès à l'information. Il ne traque pas ses utilisateurs qui bénéficient ainsi d'un

[1] Décerné par la Free Software Foundation (fsf.org)

[2] Terme pour définir le pistage des utilisateurs par les cookies d'un site web.

anonymat quasi total, peut se sentir en sécurité, sans que leurs faits et gestes soient espionnés, à des fins commerciales ou malintentionnées.

IV. LANCEURS D'ALERTE

Le *Dark Web* a permis à plusieurs lanceurs d'alerte d'exposer aux yeux du monde entier des informations sensibles, créant ainsi des polémiques.

Cependant, le *Dark Web* a aidé beaucoup de journalistes pour avoir des informations sensibles et utiles. En effet, le réseau permet au lanceur d'alerte de partager une découverte confidentielle en étant protégé de l'anonymat.

Par exemple, en 2010, avec l'affaire *Cablegate*, des documents sensibles ont été publiés sur WikiLeaks, ils contenaient des informations concernant les affaires classifiées des États-Unis. Cet épisode a soulevé plusieurs questions relatives à la transparence du gouvernement ainsi qu'aux limites de la liberté d'expression [11].

WikiLeaks, mentionné plus haut, est un site créé par Julian Assange en 2006. Ce site publie des documents officiels gouvernementaux censurés, qui regroupent plusieurs sujets, notamment « guerres » et « espionnage ». Ces informations ont pour la plupart été obtenues sur le *Dark Web.* Le fondateur de WikiLeaks est devenu une icône médiatique, reconnu lui-même comme lanceur d'alerte depuis qu'il a diffusé certains documents concernant l'armée américaine.[9][10]

V. LIBERTÉ D'EXPRESSION

Le *Dark Web* est une expérience de pouvoir et de liberté. Cependant, son utilisation en tant que plateforme de communication est fortement limitée face à la simplicité d'utilisation et à l'addiction créée par les réseaux sociaux du Web de surface (Facebook, Instagram, TikTok, Twitter). [3]

Pourtant, le *Dark Web* offre, à toute personne ayant une connexion internet, un espace pour partager des informations et exprimer ses opinions sans craindre la censure ou des représailles. [4]

Face aux craintes suscitées par la protection des données, le développement de la communication privée, anonyme ou intraçable, pourrait représenter un marché à part entière [5], [6]. Bon nombre d'applications de messagerie (Telegram, Signal, Wire, Whatsapp, Dust) implémentent déjà l'envoi de messages chiffrés. Leur taux d'adoption caractérise cette transition en marche.

Néanmoins, le *Dark Web* ne devrait pas disparaître, il fait partie du Web et reste disponible à tous. Il pourrait paraître moins utile dans les démocraties technologiquement puissantes, qui auraient réussi à opter pour des alternatives simples d'utilisation, respectueuses de la vie privée. Mais en attendant la censure ne risque pas de disparaître, laissant une place au *Dark Web*, pour la liberté d'expression.

VI. DU WEB AU DARKWEB ?

Et si le Web devenait impraticable ? Le *Dark Web* offre une alternative au Web de surface, devenu saturé, surchargé de contenu de mauvaise qualité, manipulé par des intérêts commerciaux ou encore généré par des IAs. Alors que le Web traditionnel abonde de fausses informations, le *Dark Web* pourrait retrouver son rôle initial de fournisseur d'informations de qualité.

En effet, le *Dark Web* offre une plateforme de choix pour les éditeurs qui n'ont pas besoin de surveiller constamment leur audience ou de se conformer aux réglementations telles que le RGPD. De même, il reste une alternative à considérer pour toutes celles et ceux qui cherchent à préserver la confidentialité et l'intégrité d'une information.

Il ne peut être ni détruit ni interdit, et plutôt que de lutter contre cette réalité, il semblerait bénéfique de mieux le comprendre pour en tirer parti. Certes il n'est pas exempt de défis et de risques, mais avec un peu de bon sens et de vigilance, il ne semble pas y avoir de raisons de l'ignorer. Alors, comment accéder au *Dark Web* en toute sécurité ? Le Web de surface propose quelques conseils [12].

REFERENCES

[1] UNESCO: *Le journalisme est un bien public : tendances mondiales en matière de liberté d'expression et de développement des médias ; Rapport mondial 2021/2022*, 2022 — ISBN 978-92-3-200262-4

[2] *2010 Free Software Awards announced — Free Software Foundation — Working together for free software*. URL https://www.fsf.org/news/2010-free-software-awards-announced. - consulté le 2023-06-22

[3] FRADIN ANDREA: ProPublica, „premier site d'info majeur du Dark Web" (2016)

[4] GEHL, ROBERT W: Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. In: *New Media & Society* Bd. 18, SAGE Publications (2016), Nr. 7, S. 1219–1235

[5] ARNAUD VIARD: *Les défis et conséquences du Deep Web sur notre environnement et notre économie*. Genève, Haute École deGestion deGenève (HEG-GE), Travail de Bachelor, 2017

[6] RAZORFISH: *Les Français face aux cookies*, 2022

[7] *Les 5 meilleures apps de messagerie chiffrée - Le Monde Informatique*. URL https://www.lemondeinformatique.fr/actualites/lire-les-5-meilleures-apps-de-messagerie-chiffree-65936.html. - consulté le 2023-06-22.

[8] BBC News launches „dark web" Tor mirror (2019)

[9] WIKIPEDIA: Julian Assange

[10] WIKILEAKS: What is WikiLeaks

[11] WIKIPEDIA: United States diplomatic cables leak (n.d.)

[12] Kaspersky URL https://www.kaspersky.fr/resource-center/threats/deep-web