Université de Montréal

Être visible sur et par internet : Le cas de l'État islamique

Par
Valentine Crosset

École de criminologie, Faculté des arts et des sciences

Thèse présentée en vue de l'obtention du grade de doctorat (Ph.D.) en criminologie

Février 2020

Université de Montréal
École de criminologie, Faculté des études supérieures

Cette thèse intitulée :

Être visible sur et par internet : Le cas de l'État islamique

Présentée par :

Valentine Crosset

A été évaluée par un jury composé des personnes suivantes :

David Décary-Hétu
Président-rapporteur

Samuel Tanner
Directeur de recherche

Benoît Dupont
Co-directeur de recherche

Mulone Massimiliano
Membre du jury

Xavier Crettiez
Examinateur externe

RÉSUMÉ

Cette thèse porte sur la visibilité de groupes qualifiés d'extrémistes sur internet. Si plusieurs études ont décrit les différents usages des technologies numériques par des groupes radicaux et la manière dont internet serait un catalyseur de radicalisation, peu d'études ont cherché à analyser la relation constitutive entre un dispositif technique et des militants extrémistes. L'objectif de la thèse est de renouveler le modèle de la visibilité médiatisée de groupuscules qualifiés d'extrémistes, en tenant compte des reconfigurations mutuelles entre les plateformes numériques et le groupe militant. Sur le plan théorique, cette recherche se situe à l'intersection de la théorie de l'acteur-réseau, des *software studies* et des travaux de Lucy Suchman (2007) sur les dynamiques de reconfigurations mutuelles et permanentes des relations entre humains et machines. Basée sur l'étude du cas de l'État islamique, l'analyse s'ancre dans des données provenant d'un terrain de recherche de type ethnographique, collectées sur un an et demi. L'enquête est composée d'une observation non participante menée sur plusieurs plateformes numériques exploitées par le groupe jihadiste, de l'archivage et l'analyse des traces en ligne, ainsi que d'un corpus documentaire.

Nos résultats contribuent premièrement à une meilleure compréhension de la visibilité des groupes qualifiés d'extrémiste sur les plateformes numériques, en démontrant qu'elle est relationnelle, technicisée et conflictuelle. Notre étude fait tout d'abord ressortir qu'on assiste à une complexification du tableau de la visibilité. La visibilité en ligne de l'État islamique nécessite un vaste réseau d'acteurs, tels que spécialistes des médias, militants, spécialistes en cybersécurité et *botnets*. La visibilité mêle ainsi des procédés hors-ligne et en ligne, décentralisés et centralisés. L'analyse des pratiques quotidiennes de visibilité montre que le travail d'apparence des militants de l'État islamique suit un objectif d'amplification et d'abondance de leur flux informationnel. Le but est d'inonder les plateformes de réseaux sociaux de contenus pro État islamique, afin de mener une « guerre médiatique ». Par ailleurs, les résultats suggèrent que la visibilité est complexe en raison des séries de contraintes et de forces ennemies qui contrecarrent le projet en ligne de l'État islamique, tel que la modération de leurs contenus. Parallèlement, notre étude montre que la présence de ces usagers a redessiné la régulation de ces technologies en les rendant plus contraignantes. Enfin, nos résultats dévoilent que les militants de l'État islamique refusent l'assujettissement face aux suspensions répétées dont ils font l'objet. Pour limiter les effets négatifs de la modération, le collectif travaille activement à mettre en place des tactiques de résistance.

Dans un second temps, la thèse s'intéresse aux formes de visibilité que cette médiation technique entre les militants et les plateformes numériques configure. Nous proposons le concept de *visibilité technicisée* pour rendre compte de la visibilité en ligne des opinions politiques. Ce type de visibilité se fonde sur l'incessant déploiement d'une raison technique. En cela, la visibilité devient une activité spécialisée qui exploite les dimensions techniques et automatisées des technologies numériques, avec leurs normativités propres. Si la visibilité technicisée confère aux utilisateurs du pouvoir pour assurer leur visibilité, la thèse émet certaines réserves quant à la valeur réelle de ce faire-voir. Elle montre que, dans la quête d'efficacité et d'abondance qui la caractérise, ce type de visibilité technicisée généralise un ensemble de comportements nuisibles et de procédures trompeuses pour exprimer une opinion politique. Révélatrices de nouvelles formes de domination et d'asymétrie, nous plaidons qu'elle pourrait à terme contraindre le jeu démocratique.

Mots-clés : visibilité – plateformes numériques – internet – militantisme – extrémisme – État islamique –reconfiguration – technique.

SUMMARY

This thesis focuses on the visibility of extremist groups on the internet. While several studies have focused on describing the different uses of digital technologies by radical groups and the way the internet would operate as a catalyst for radicalization, few studies have sought to analyze the constitutive relationship between the technical apparatus and the militant extremist. The objective of the thesis is to renew the visibility model of groups classified as extremists, taking into account the mutual reconfigurations between digital platforms and the militant groups.

At a theoretical level, our study is situated at the intersection of actor-network theory (ANT), *software studies* and Lucy Suchman's work (2007) on the *dynamic reconfiguration of mutual and permanent* relationships between humans and machines. Based on the case study of the Islamic State, this analysis, lasting one and a half years, was anchored in data from an ethnographic research field. The survey consists of non-participant observation of several digital platforms exploited by the jihadist group, online archiving and analysis of online traces, as well as a documentary corpus.

Our results contribute to better understanding how groups qualified as extremist develop their visibility on digital platforms, by emphasizing that it is relational, technical and conflictual. First of all, our study demonstrates the evolution to a more complex development of the resources used to obtain visibility. The online visibility of the Islamic state requires a vast network of actors, such as media specialists, activists, cybersecurity specialists and *botnets*. For this reason, offline and online, decentralized and centralized processes are combined. The analysis of their daily practices shows that the work of Islamic state militants to obtain visibility strive at amplification and abundance of their information flow. Their goal is to inundate social media platforms with their contents, conducting a "media war". Furthermore, the results obtained suggest that developing visibility is complex due to a series of constraints and enemy forces that thwart the Islamic State project, such as moderation of contents as an example. At the same time, our study shows that the presence of this type of users has resulted in the redesign of the regulation of these technologies, making them more restrictive. Finally, the results reveal that the Islamic state militants are actively working to put in place resistance tactics in order to limit the negative effects of that moderation.

In a second step, the thesis focuses on the forms of visibility evolving from this technical mediation between activists and digital platforms. We suggest the concept of *technical visibility* to highlight the online visibility of political opinions. This type of visibility is based on the deployments of a technical rationality. Therein the creation of visibility becomes a specialized activity using the technical as well as mechanized dimensions of digital technologies, each with their own mode of normativity. If technical visibility gives users the possibility to develop their visibility, the thesis expresses certain reservations as to the real value of this *"faire-voir"*. It shows that this type of *technical visibility*, due to its characteristic quest for efficiency and abundance of information, generalizes bulk, aggressive, or deceptive activity. This results in new forms of domination and asymmetry. We therefore argue that it could jeopardize democracy.

Key-Words: visibility – digital platforms – internet – activism – extremism – Islamic State – reconfiguration – technical.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

REMERCIEMENTS

Il serait illusoire de penser qu'une thèse de doctorat s'écrive seul, tant celle-ci se réalise et s'aboutît grâce aux nombreuses personnes sur lesquelles les doctorant.e.s peuvent compter tout au long de son parcours. J'aimerais donc par ces quelques lignes exprimer ma reconnaissance à toutes ces personnes qui m'ont aidée à mener à bien cette thèse.

Pour commencer, je souhaite profondément remercier mes directeurs, Samuel Tanner et Benoît Dupont, pour leur soutien infaillible tout au long de mon parcours doctoral. Il me serait impossible de leur exprimer ici toute ma gratitude pour m'avoir permis de développer mes idées avec la plus grande des libertés, pour les innombrables discussions éclairantes, mais aussi pour m'avoir guidée dans mes nombreux moments d'incertitude et de doute. Samuel, merci de m'avoir donné le goût pour la théorie à travers nos échanges et le séminaire de doctorat, qui aura été une riche source d'inspiration. Aussi, merci de m'avoir accordé ta confiance en tant qu'assistante de recherche pendant plus de quatre ans. Benoît, il va sans dire que tu m'as transmis le goût pour les nouvelles technologies et pour internet. Nos interactions m'auront permise d'en connaître toujours plus, mais surtout d'aiguiser mon regard critique sur ces questions. Je te remercie aussi d'avoir toujours été attentif à m'apprendre les nombreuses « ficelles » du métier.

Il importe d'admettre que le Département de criminologie de l'Université de Montréal a constitué un environnement de travail des plus propices pour mener ma thèse. Au sein du Département, j'ai notamment eu la possibilité d'enrichir mes réflexions en échangeant avec les professeur.e.s et les étudiant.e.s. Je tiens tout spécialement à remercier Anthony Amicelle, Jean Bérard et Karine Côté-Boucher qui ont commenté mon travail à différents moments de mon parcours au travers de conversations enrichissantes. Je remercie également Étienne Blais pour son enthousiasme concernant mon projet de thèse et ses nombreux commentaires lors du séminaire de thèse. Merci aussi à mes collègues étudiant.e.s pour les échanges que nous avons eus lors de séminaires, dans les couloirs ou encore au CyberLab. Merci à Elsa pour ces longues discussions que nous avons menées dans nos bureaux ou autour de cafés. Plus particulièrement, je tiens à remercier Rosalie, Sabrina, Annie et Killian qui en plus d'être des collègues hors pairs, sont d'extraordinaires amis.

Et puis, il y aussi ces étudiant-es qu'on rencontre dans d'autres départements et qui contribuent fortement à faire mûrir nos réflexions. Merci à Nathalie et à Camille pour toutes ces discussions houleuses sur l'intelligence artificielle et tous les non-humains de ce monde. Mes remerciements s'adressent également aux personnes qui ont pris le temps de relire minutieusement ma thèse. Merci à Camille pour ses innombrables commentaires d'une grande perspicacité. Merci aussi à Alexis pour ses précieux commentaires. Merci également à son œil aiguisé qui a passé au crible les potentielles coquilles. Je vous dois beaucoup. Sans vous, il m'aurait été difficile de mettre une fois pour toutes un point final à cette thèse.

Je me dois aussi de remercier le Fonds de recherche du Québec – Société et culture, l'École de criminologie, le Centre d'études et de recherches internationales et la Faculté des études supérieures et postdoctorales de l'Université de Montréal pour les bourses octroyées pendant mes années d'études. Un merci spécial pour le Fonds de recherche du Québec – Société et culture, qui a ouvert son concours aux étudiants étrangers en 2017 et qui m'a permis de terminer mes études dans les meilleures conditions possible. Je tiens aussi à exprimer ma gratitude et ma reconnaissance aux membres du personnel administratif de l'École de criminologie et du CICC. Martine, Geneviève et Caroline, merci pour votre bonne humeur quotidienne et votre bienveillance sans borne à l'égard des étudiant-es. Merci aussi à Nicole et à Marc pour leur travail et pour répondre à nos innombrables demandes, souvent pressantes.

Merci également à ma famille et à mes ami.e.s qui m'ont continuellement soutenue durant cette thèse et grâce à qui je me suis octroyée ces moments de lâcher prise chers aux doctorant.e.s. Merci à mes parents, Anne-Marie et Robert, pour leur support moral au quotidien qu'ils m'ont toujours apporté malgré les milliers de kilomètres qui nous séparaient. Vous avez su faire preuve, une fois de plus, d'une grande générosité et de bienveillance. Merci à mes sœurs Géraldine et Marie, ainsi qu'à mon frère Benoît avec lesquels j'ai pu déconnecter de ma thèse durant de brefs moments. Comme depuis toujours, vous avez toujours répondu sans faille à votre poste de grande sœur et de grand frère quand il le fallait. Merci à ma tante Marie-Claire pour sa curiosité et pour ses nombreuses relectures de mes écrits en anglais. Et puis, il y a aussi ces ami.e.s qu'on laisse de l'autre côté de l'Atlantique et qui vous rappellent ô combien il est temps de remettre cette thèse ! Merci à Phénicia, Lola, Isis, Fanny, Laurie d'avoir toujours étées là. Merci aussi à Eloïse. Faire cette thèse loin de

vous tous aura sans doute été la chose la plus difficile, mais vous êtes sans hésitation les meilleurs appuis qu'on puisse avoir à distance.

Merci finalement à mon amour de toujours, Xavier, qui a été l'un des piliers principaux tout au long de ce parcours. Il me serait extrêmement ardu de résumer en quelques lignes le support indéfectible dont il a fait preuve durant ces cinq années et demie. Sans cette présence affectueuse, il m'aurait toutefois été difficile d'arriver au bout de cette thèse. Xavier, merci d'avoir rendu la route du doctorat plus douce et plus joyeuse, pour ta patience sans limite, mais aussi de m'avoir donné le courage et la persévérance nécessaire pour continuer dans mes grands moments de doute. Merci aussi pour ton soutien sur le plan intellectuel, en étant toujours à l'écoute de mes idées et prêts à débattre inlassablement. Tu as été la personne la plus précieuse durant toutes ces années.

AVANT-PROPOS

Le Monde 2014[1]. Je lis dans le quotidien que des jeunes adolescents occidentaux échangent sur les réseaux sociaux Twitter et Instagram des images d'atrocités commises en Syrie. On apprend que « l'irruption des médias sociaux dans les conflits est en train de changer le visage de la guerre dans les sociétés occidentales ». Pour l'auteur de l'article : « la guerre est désormais à portée de main ou d'un clic ». Ce à quoi, il ajoute quelques paragraphes plus loin que « de toute façon, Al-Qaïda n'avait plus de propagandistes : avec le 11 septembre, Oussama Ben Laden est devenu une "marque" internationale. L'internet suffisait, il est devenu le théâtre du deuxième temps du jihad mondial. Les sites extrémistes ont fleuri, permettant d'abolir les frontières et de sauter les océans ».

Voici donc une saisissante illustration des dystopies contemporaines qui entourent le terrorisme et les technologies numériques. Replaçons le contexte. Par l'effet de la recrudescence de jeunes occidentaux partis faire le jihad en Syrie et en Irak, internet a régulièrement été blâmé pour son rôle dans la radicalisation. Le ton était donné : la technique serait au service d'un extrémisme violent. C'est en pareilles circonstances que les géants du web ont été mis sur le banc des accusés. Les injonctions des gouvernements se sont multipliées. Les géants du web doivent modérer les contenus plus abondamment et plus agressivement. Ils ont maintenant des comptes à rendre. Et face à cela, les plateformes n'ont que deux solutions : réagir ou se murer dans le déni, avec pour risque qu'à terme cela nuise à leur réputation et à leur image. D'ailleurs, les réactions des acteurs privés envers la prolifération des contenus jihadistes ont été diverses et ont évolué au cours du temps (Ducol, 2015). Par exemple, si Facebook et YouTube ont rapidement réagi, Twitter a longtemps maintenu l'une des politiques de liberté d'expression les plus tolérantes. Ce dernier a effectivement affiché une position farouchement neutre à l'égard des contenus touchants l'État islamique, ce jusqu'aux vidéos montrant la décapitation de James Foley.

Le fait que les technologies du web soient pointées du doigt dans le contexte des transformations du terrorisme n'est pas nouveau (Conway, 2007 ; Ramsay, 2008). On se rappelle que les années 1990 ont montré une inquiétude grandissante face aux risques d'attaques cyberterroristes. Une tendance qui a perdu son souffle à la suite du 11 septembre

[1] « Le djihad 3.0 », 23 avril 2014, voir : https://www.lemonde.fr/idees/article/2014/04/23/le-djihad-3-

2001. Ce que les attentats du 11 septembre ont révélé à cet égard, c'est qu'Al-Qaïda n'a pas fait un usage de type futuriste ou avancé des technologies numériques (Ramsay, 2008). Pour Ramsay, le 11 septembre « was not a technological coup, but an organisational one » (2008 : 4). Finalement, les auteurs d'actes terroristes n'entretenaient qu'un lien léger avec le cyberterrorisme.

Résumons. Avec la présence de l'État islamique sur les réseaux sociaux, de nouvelles craintes ont fait surface : celles de la radicalisation « expresse » des militants par le biais d'internet. Sans conteste, les géants du web ont été mis à rude épreuve face à la prolifération de flux informationnels jihadistes. Tout au long de mon enquête, j'ai pu voir que cette diffusion était devenue un enjeu politique majeur. Les attentats répétés en Occident et le départ pour la Syrie et l'Irak de jeunes occidentaux ont contribué à provoquer une vaste mobilisation pour contrer la propagande jihadiste sur internet. Sécuriser internet était devenu l'une des conditions de garantie de la sécurité nationale. Par ailleurs, ces internautes jihadistes sont venus toucher l'une des valeurs clés de la Silicon Valley : la liberté d'expression.

Dans ce contexte, j'en suis venue à me demander comment ce type d'utilisateur emploie ces technologies au quotidien pour assurer une visibilité. En réalité, nous en savons très peu sur les pratiques en ligne des militants appartenant à des groupes qualifiés d'extrémistes. Il est donc apparu nécessaire de marquer un temps d'arrêt et de prendre le temps d'ouvrir la « boîte noire » de cette nouvelle médiation technique et d'en étudier le fonctionnement. Il ne s'agit donc pas d'une thèse sur la radicalisation. Ce qui anime cette thèse est, au contraire, d'aller au-delà, voire à l'encontre des conceptions qui dominent l'espace public sur le sujet, c'est-à-dire de dépasser les conventions qui marquent le discours sur la radicalisation en ligne.

Introduction

Au milieu des années 1990, internet a posé la question de la mondialisation et de l'évolution technique de la menace terroriste, jusque-là souvent associée à un territoire géographiquement délimité (Bonditti, 2005). Si la recherche s'est d'abord focalisée sur de potentielles attaques cyberterroristes, les chercheurs se sont aperçus que les auteurs d'actes terroristes faisaient un usage assez conventionnel des technologies numériques (Ramsay, 2008). Ce constat établi, le caractère polémique de l'utilisation des technologies numériques par des groupes radicaux s'est ensuite construit autour de la crainte qu'elles puissent jouer un rôle dans la radicalisation des jeunes candidats au jihad. Notre objectif n'est pas de discuter de la pertinence de cette accusation. Toujours est-il qu'après les attentats de Londres en 2005, cette inquiétude a causé une vaste mobilisation de lutte contre la propagande jihadiste sur internet. Les autorités publiques de pays touchés par des attaques ont soulevé le danger que pouvaient représenter des technologies permettant à des groupes qualifiés de terroristes de propager leur propagande et leurs stratégies opérationnelles, de recruter ou encore de lever des fonds. Dès ce moment, sécuriser internet est devenu l'une des conditions pour assurer la sécurité nationale.

L'utilisation d'internet par des groupuscules qualifiés d'extrémistes[2] a fait l'objet d'une littérature abondante. Le réductionnisme technique a souvent été de mise pour expliquer comment ces groupes utilisent internet. Ces travaux considèrent que les technologies numériques sont neutres dans la mesure où elles satisfont simplement une fin. Internet est ainsi cantonné au statut d'outil qui sert les groupes extrémistes à partager des informations, à collecter des fonds, à recruter ou encore à planifier et coordonner des actions (Awan, 2007b ; Bockstette, 2009 ; Denning, 2010 ; Gates et Podder, 2015 ; Rudner, 2017 ; Tsfati et Weimann, 2002 ; Weimann, 2004, 2016 ; Whine, 1999). Dans la même lignée, un autre ensemble d'études ont pour leur part affirmé la crainte qu'internet puisse jouer un rôle majeur dans la radicalisation des individus (Awan 2007a, 2007b ; Cole, 2012 ; Conway, 2012, 2014 ; Edwards et Gribbon, 2013 ; Gill et al., 2015 ; Huey, 2015 ; Omotoyinbo, 2014 ; Pearson, 2016 ; Von Behr et al., 2013). Ce qui tend à limiter la portée de l'ensemble de ces études est

[2] Pour éviter l'embarras normatif que le terme extrémisme comporte, nous considérerons dans cette thèse qu'il s'agit de groupes *qualifiés* d'extrémistes ou de terroristes. Pour des raisons de concision, nous utiliserons parfois directement la terminologie terroriste ou extrémiste, n'enlevant en rien son caractère construit. Nous renverrons aussi ces groupes à des termes plus généraux tels que ceux de militantisme et d'activisme. Cette posture est explicitée plus avant dans l'introduction de la section 4.1. de notre méthodologie.

qu'elles situent la technique comme une force autonome dont il suffirait d'étudier les effets sur les groupes militants.

D'autres études, logées en communication, ont étudié l'appropriation des technologies numériques par ces groupes en portant leur attention sur les *affordances* numériques (Baugut et Neumann, 2019 ; Caiani et Wagemann, 2009 ; De Koster et Houtman, 2008 ; Ernst et al., 2017 ; Evolvi, 2019 ; Gattinara et Bouron, 2019 ; Krämer, 2017 ; Marwick et Lewis, 2017). Se distinguant de l'instrumentalisme caractéristique des approches précédentes, ces études ont le mérite de restituer la complexité des technologies numériques dans l'analyse du phénomène. Aussi stimulants qu'ils soient, ces travaux présentent le risque de sur-interpréter le médium, négligeant par là les effets que ces groupes pourraient avoir sur ces technologies.

Dans un cas comme dans l'autre, la question de la co-constitution entre technologie et groupe extrémiste reste à poser et à examiner. L'intention générale de cette thèse est d'aborder les liens qui se tissent entre des groupes qualifiés d'extrémistes et un dispositif technique, en l'occurrence des plateformes numériques, à des fins de visibilité. Les questions de recherche qui nous occupent sont les suivantes : (1) comment s'articule la relation entre un dispositif technique et un groupe qualifié d'extrémiste et (2) quelles formes de visibilité cette co-constitution configure-t-elle ? Nous aborderons la visibilité de ces groupes en la recadrant dans un processus de reconfiguration mutuelle entre les technologies numériques et les militants. Pour ce faire, nous concentrerons notre attention sur la visibilité en ligne du groupe État islamique[3]. L'État islamique est particulièrement reconnu pour avoir galvanisé les plateformes de réseaux sociaux. Le groupe a effectivement rapidement compris l'importance d'internet. Il a développé une visibilité efficace en misant autant sur la qualité que sur la quantité des contenus offerts à des audiences mondialisées (Atwan, 2015 ; Awan, 2017 ; El Difraoui, 2016 ; Koerner, 2016 ; Singer et Brooking, 2018 ; Winter, 2015). Simultanément, son usage des plateformes numériques a été la cible de tous les débats et inquiétudes, obligeant les géants du web à lutter contre ce type d'acteurs. Les militants ont ainsi été voués à une requalification : ils n'étaient plus de simples usagers, mais étaient devenus des usagers « indésirables » à exclure.

[3] Voir Annexe 1 pour une brève introduction à la genèse de l'État islamique.

Le cas de l'État islamique nous semble constituer un formidable laboratoire pour envisager les reconfigurations mutuelles qui se forment entre un dispositif technique et un militant, ainsi que les nouveaux enjeux liés à la visibilité en ligne. Le lecteur l'aura compris : le but de cette thèse n'est pas de faire une analyse sur le jihadisme. Il n'est pas non plus question de fétichiser l'objet technique. Notre intérêt spécifique pour la visibilité de groupes militants, qui plus est qualifiés d'extrémistes, s'attache à la manière dont la technique et le militant tissent des liens qui conduisent à des formes de visibilité et d'invisibilité. Cet intérêt particulier diffère des études existantes sur le militantisme en ligne et l'extrémisme.

La thèse comporte neuf chapitres. Le premier chapitre procède à une analyse critique de la littérature. Elle s'articule au constat de situer la visibilité des groupes militants dans toute la complexité qu'elle recèle, c'est-à-dire en dépassant un vocabulaire dualiste : anciens/nouveaux médias, hors-ligne/en ligne, humain/technique. La première section se consacre à la spécification de la notion de visibilité, en particulier lorsque celle-ci résulte d'une médiation technique. La seconde partie porte plus spécifiquement la question de la visibilité aux mouvements sociaux. La troisième partie revient sur les recherches qui ont abordé la relation entre les médias et les mouvements radicaux. La quatrième section se penche plus spécifiquement sur le rôle d'internet dans les mobilisations. Cette section insiste notamment sur la nécessité de restituer le militantisme dans une interaction complexe entre le numérique et le non numérique. Enfin, la dernière section s'intéresse aux stratégies de visibilité de notre cas à l'étude, l'État islamique.

Le deuxième chapitre prolonge la question de la complexité soulevée dans le premier chapitre, en portant une attention plus particulière au contexte socio-technique au sein duquel se joue la visibilité des militants, à savoir le web 2.0. Ce chapitre commence par une revue des différents travaux ayant approché la question du rôle d'internet dans les transformations de l'espace d'apparence. La deuxième section décrit les fondations techniques des technologies. Il spécifie notamment la manière dont les architectures techniques formatent différents *designs* de visibilité. La troisième section s'intéresse quant à elle aux multiples couches techniques qui composent les technologies numériques. Après avoir fait le point sur les dimensions techniques, la dernière section porte sur la modération en ligne et pose la question de la régulation sur internet. Nous verrons que la modération se distribue au sein de différents acteurs : la communauté en ligne, les plateformes numériques et les pouvoirs publics. L'ensemble du chapitre permet ainsi une première amorce du rôle des non-humains

(codes, algorithmes, protocoles, plateformes, etc.) dans le fonctionnement de la visibilité en ligne.

Le troisième chapitre expose le cadre conceptuel que nous mobilisons dans l'analyse de la visibilité en ligne de l'État islamique. Notre posture théorique s'inspire de la sociologie de l'acteur-réseau, des *software studies* et des travaux de Suchman (2007) sur les dynamiques de reconfigurations mutuelles des relations entre humains et machines. L'articulation de ces différentes théories en un cadre unifié nous incite à voir la visibilité médiatisée sous l'angle d'une perspective *matérielle-sémiotique*. Cela renvoie à l'idée que : 1) la visibilité médiatisée doit s'envisager comme une relation d'entités humaines et non-humaines ; 2) ces entités se reconfigurent mutuellement ; 3) elles s'accompagnent de mouvements et de mutations ; 4) la visibilité médiatisée doit être située dans son contexte socio-technique.

Le quatrième chapitre présente la méthodologie. Comme mentionné plus haut, notre approche méthodologique s'appuie sur l'étude de la visibilité en ligne de l'État islamique. C'est par l'observation en ligne que le matériel central de cette thèse a été constitué. Ce matériel s'accompagne d'une documentation comprenant trois types de sources : les documents produits par les protagonistes de l'État islamique, les documents qui visent à faire « parler » l'objet technique et le matériel documentaire périphérique – tel que des documents législatifs et des articles de presse. Après avoir présenté nos choix et approches méthodologiques, nous retraçons notre itinéraire de recherche de manière réflexive et critique. C'est ainsi que nous spécifierons les étapes de la cueillette de données, les méthodes d'enquête retenues et les caractéristiques du terrain étudié. Nous formulerons également quelques remarques quant aux limites inhérentes à un terrain sur internet et défini par lui, mais aussi quant aux questions éthiques qui marquent ce type de terrain.

Les chapitres 5, 6, 7 et 8 sont consacrés à l'analyse de nos données empirique. L'objectif du chapitre 5 est de suivre les premières tentatives visant à lier concrètement le dispositif technique et le collectif jihadiste. Plus concrètement, ce chapitre saisit les prémisses du programme d'action de cette nouvelle médiation technique. La première section expose les récits et métaphores de l'État islamique à l'encontre d'internet. La seconde montre que l'action de visibilité est distribuée au sein d'un collectif hybride composé de spécialistes de médias, de militants, de *botnets* et de spécialistes en cybersécurité. La troisième section rend compte des règles et des normes communes, parfois implicites, pour mener à bien la mission

de visibilité. La dernière partie décrit la façon dont les militants de l'État islamique théâtralisent leurs compétences techniques. En somme, ce premier chapitre d'analyse fait ressortir la complexité qui sous-tend l'organisation de la visibilité des militants de l'État islamique et la manière dont ces derniers associent internet à un front de bataille.

Le chapitre 6 décrit comment le collectif capte l'attention de ses adversaires et de ses partisans par le biais d'opérations offensives, trompeuses et effectuées en masse. Ce chapitre soutient que la visibilité de l'État islamique s'inscrit dans un programme d'amplification et d'abondance de leurs contenus. Le but étant d'envahir les plateformes le plus massivement possible. Notre enquête montre que cet objectif revendiqué par le groupe se traduit par un ensemble de comportements nuisibles et de procédures douteuses (*spammer*, *troller*, harceler ou encore créer de fausses amplifications). Nous commencerons pas décrire la manière dont le collectif articule sa narration au sein de mèmes, pour attirer plus efficacement l'attention. Ensuite, nous nous attarderons plus spécifiquement aux stratégies d'amplification utilisées par les militants de l'État islamique. Enfin, ce chapitre contribue à montrer comment cette logique d'amplification et d'abondance configure de nouvelles formes de combats entre adversaires, notamment par l'automatisation de réseaux de *botnets* qui s'affrontent dans des luttes iconographiques et énonciatives de grandes ampleurs.

Le chapitre 7 porte sur les anti-programmes qui tentent de contrer le projet de visibilité en ligne des militants de l'État islamique. Ce chapitre se consacre aux questions de modération des contenus, comme frein au travail de diffusion du collectif. Le chapitre commence par exposer les nouvelles législations et les nouveaux règlements qui visent à encadrer plus sévèrement la diffusion des contenus radicaux et terroristes sur internet. Après ces précisions, la deuxième section approfondit la manière dont la modération se réorganise au sein des plateformes. Ensuite, est décrit le vaste réseau d'acteurs humains et non-humains nécessaires au fonctionnement de la modération. La dernière section aborde la façon dont des internautes s'approprient le devoir moral de lutter contre les militants jihadistes, en recourant à des signalements massifs. Nous verrons par ailleurs dans cette section comment les militants de l'État islamique ont procédé à un nouveau positionnement stratégique, pour contenir ces menaces. Ce chapitre permet d'approfondir les reconfigurations qui s'opèrent lorsqu'un usager indésirable s'approprie un dispositif technique. Dans notre cas, il s'agit de démontrer le renfoncement du dispositif socio-technique de la modération. De plus, ce chapitre contribue

à montrer un changement dans la logique de signalement : de moyen de protection de la communauté, le signalement devient une arme de combat pour faire taire l'adversaire.

Le chapitre 8 rend compte des tactiques de résistance que les militants de l'État islamique ont mises en place pour assurer leur survie en ligne face aux modérations répétées. Ce chapitre passe en revue ces différentes tactiques, ainsi que la manière avec laquelle les militants de l'État islamique contestent la modération dont ils font l'objet. Cette partie de la thèse renvoie finalement à l'incapacité des plateformes numériques à discipliner l'utilisation. Le chapitre s'attarde effectivement à montrer comment la modération reconfigure les usages des militants de l'État islamique vers des tactiques qui visent à perpétuer leur flux informationnel. Les deux dernières sections détaillent deux types de configurations d'usager dans le contexte répété des modérations : l'*usager martyre* et l'*usager trompeur*.

Enfin, dans le dernier chapitre, la conclusion générale, nous effectuerons une synthèse des principaux enseignements tirés de notre étude de cas. Le fil conducteur de la thèse consiste à montrer que la visibilité de l'État islamique est relationnelle, technicisée et conflictuelle. Cette section opère un retour sur nos résultats à partir de trois notions essentielles de notre cadre conceptuel : l'assemblage, l'action et la reconfiguration. Elle vise ainsi à une meilleure compréhension des liens qui se tissent entre les militants de l'État islamique et les plateformes, à des fins de visibilité. Dans un deuxième temps, nous introduirons et détaillerons le concept de *visibilité technicisée*. Nous proposons l'idée suivant laquelle la visibilité sur internet se fonde sur un incessant déploiement d'une raison technique, qui s'apparente à une série de comportements nuisibles et trompeurs. À la suite de cette proposition, nous soulignerons nos principales contributions. Celles-ci se situent au carrefour des études sur l'activisme en ligne, la visibilité et les plateformes numériques et consistent explicitement à apporter un nouvel éclairage sur la visibilité en ligne des groupes militants. Enfin, nous terminerons en évoquant quelques-unes des pistes de recherche ouvertes par nos travaux.

PARTIE I :

Visibilité, activisme et technologies de communication

Chapitre 1 : Activisme et visibilité

Ce premier chapitre a pour objectif de présenter la revue de littérature liée à notre objet de recherche. Elle se décline en cinq parties. Notre première section se consacre à la spécification du concept central de notre thèse, la visibilité médiatisée. Face à l'abondance des sources intéressées par le thème de la visibilité, l'ambition ne sera pas de les épuiser, mais d'en dresser le portrait. Suivra une deuxième section, consacrée à la visibilité des mouvements sociaux. Elle introduira d'abord la sociologie des mouvements sociaux pour s'intéresser ensuite à la relation entre la visibilité, les médias et le militantisme. Dans la troisième section, nous introduirons les travaux qui se sont intéressés à l'activisme extrémiste, à leurs stratégies de communication et à leur rapport aux médias. Cette section se terminera en insistant sur la nécessité de dépasser la dichotomie traditionnelle entre nouveaux et anciens médias. Dans la quatrième section, nous nous intéresserons à la sociologie des mouvements sociaux et à l'activisme en ligne. Enfin, la dernière section met en perspective l'usage d'internet par la mouvance salafiste-jihadiste, et plus particulièrement par l'État islamique. En guise de conclusion, nous verrons qu'il importe de restituer notre objet de recherche dans toute sa *complexité*. Celle nécessite d'éviter de tomber dans le piège de l'utopisme ou de la dystopie numérique, ainsi que dans celui des dualismes traditionnels (anciens/nouveaux médias, hors-ligne/en ligne, humain/technique).

1.1. Définir et situer la visibilité médiatisée

La visibilité ne fait pas l'objet d'une seule conversation (Brighenti, 2007). Si elle s'ouvre à un large champ réflexif, c'est parce que les questions associées à cette notion se sont imposées dans beaucoup de disciplines en sciences sociales. Précisément parce que chaque discipline a eu tendance à considérer la visibilité comme un concept local (Brighenti, 2007), les débats définitionnels sont infinis. Cette difficulté est d'autant plus forte, du fait que les questions relatives à la visibilité renvoient à une série de concepts tels que la vision, la visualisation, la représentation ou l'image, qui font chacun l'objet d'une littérature considérable (Voirol, 2005a). On l'aura compris, la question de la visibilité occupe un champ de recherche vaste, dont il serait difficile de dresser tous les contours. Dans ce qui suit, nous retracerons brièvement les débats sur la vision qui ont animé la littérature. Ensuite, il s'agira de tenter, en partant des travaux de Brighenti (2007, 2010), de définir ce qui intéresse ou regarde la question de la visibilité. Enfin, nous terminerons cette section en accordant notre attention aux formes de visibilités qui ont émergé avec l'avènement des nouvelles technologies de communication.

1.1.1. Les contours de la visibilité

La notion même de visibilité est culturellement spécifique et historiquement située. Dans la tradition philosophique allant de Platon à Descartes, la vision a longuement été considérée comme la cause suprême du savoir[4]. L'imaginaire moderniste, incarné principalement par le perspectivisme cartésien, a pensé un modèle de la vision qui sous-tend un « voir rationaliste ». Dans cette perspective, si la vision permet un accès privilégié à la connaissance du monde, la vue n'est fiable que dans la mesure où elle se calque sur un mode de fonctionnement rationaliste (Brighenti, 2010). Le postmodernisme diverge nettement sur la question de la relation entre voir et savoir, pour eux : « the modern relation between seeing and true knowing has been broken » (Rose, 2001 :8). Néanmoins, le postmodernisme restitue

[4] Il existe toutefois des différences marquées au sein du courant philosophique. Si Platon considère dans *Timée* la vision comme le « plus noble des sens », un examen plus attentif de la célébration de la vue par ce dernier nuance une représentation trop unidimensionnelle de l'occulocentrisme grec (Jay, 1993). Platon a émis de nombreuses réserves quant à la fiabilité des yeux dans la perception réelle du monde (par exemple dans le Mythe de la caverne), marquant d'une certaine façon son incertitude quant à la valeur de la perception réelle. Lorsque Platon parle de vision, c'est celle de « l'œil de l'esprit » qui affecte notre vision, notre perception et notre intelligibilité du monde. Ainsi, « we see *through* the eyes, he [Platon] insisted, not *with* them » (Jay, 1993 :27). Descartes dans *La Dioptrique* place le champ de la vision dans une perspective mathématico-géométrique où l'œil méthodique du rationaliste permettra d'éclairer l'expérience sensorielle descriptive et l'accès à la connaissance du monde. C'est sans doute dans cette réarticulation du savoir et du voir rationaliste que les modernes se démarqueront des prescriptions faites par Platon à propos de la vision (Birghenti, 2010).

clairement l'occulo-centrisme propre à la tradition occidentale, mais cette fois-ci en dévoilant la manière dont nous sommes davantage en interaction avec des expériences visuelles construites[5]. À ce titre, Mirzoeff soutient ouvertement que le postmodernisme est une culture visuelle[6] (1998).

La tradition intellectuelle française du XXe siècle a quant à elle jeté un regard critique sur l'objet de vision, en dépeignant une réalité anti-occulocentrée (Jay, 1993). Il incombait à ces travaux de déposséder la vision de son sens suprême, en la mettant sur le mode du dénigrement, de la contrainte et des dangers. Tentant une position résolument critique, ces travaux ont considérablement modifié les modèles de la vision qui ont dominé la pensée européenne depuis Platon. Dans l'éventail de ces travaux, la production de leur critique à l'égard de l'objet de la vision est analysée à partir de positions et de perspectives très différentes. Voyez par exemple comment l'expérience d'être objet du regard de l'autre ou de son propre regard a été dépeint par la philosophie, la psychanalyse et la phénoménologie dans un double mouvement aux contours contradictoires : celui d'être source d'objectivation du soi tout en contribuant à sa propre déperdition.

Dans un autre registre, en décrivant le modèle architectural du panoptique inventé à la fin du XVIIIe siècle par Jeremy Bentham, Foucault (1975) montre les effets normalisateurs du regard disciplinaire. Foucault vise à décrire dans l'observation des conduites de surveillance, ce moment où la visibilité s'infléchit en source de domination, d'imposition de conduite et de moyen de contrôle. Dans sa critique de la société du spectacle, le situationniste Guy Debord (1968) démontre comment se dévoile l'idéologie marchande par l'imbrication du politique et du médiatique dans la sphère du spectacle et comment elle deviendra source d'aliénation. On peut également retrouver l'argumentaire de Baudrillard (1981), selon qui la postmodernité se caractérise par un recouvrement du réel sous le Virtuel, d'une perte de principe de réalité. Simulacre, Simulation, Hyper-réalité, ces mots qualifient chez Baudrillard le fait même d'un régime scopique dominé par une indistinction entre le réel et l'irréel.

[5] De nombreux travaux en anthropologies ont critiqué cette primauté du visuel tant chez les modernes que les postmodernes, en appelant à restituer la vision ainsi que la montée des technologies visuelles dans un contexte historique et géographique. L'anthropologie nous apprend qu'il existe des variations radicales dans la hiérarchisation des sens et les manières de connaître selon les cultures et les époques (voir par exemple Jay et Brennan, 1996 ; Classen, 1993, 1997 ; Hamburger, 1997 ; Howes, 1991 ; Shohat et Stam, 1998).

[6] Par culture visuelle l'auteur entend tous les événements visuels « in which the user seeks information, meaning or pleasure in an interface with visual technology » (Mirzoeff, 2002 :5).

Bien que ces exemples soient loin d'être exhaustifs, les perspectives présentées proposent des façons très différentes de comprendre la visibilité et la vision. Vacillant entre des conceptions occulo-centrées et anti-occulocentrées, nous pouvons conclure que la visibilité est un phénomène pluriel et paradoxal qui peut être compris tant sur le modèle de l'autonomisation et que sur celui l'aliénation. Ce bref panorama posé, il nous reste à élucider la question de savoir : qu'est-ce que la visibilité ?

Face à la disparité des répertoires théoriques et des registres métaphoriques de la visibilité, Brighenti (2007, 2010) plaide pour que la visibilité soit traitée comme une catégorie et un processus social à part entière. La visibilité ne peut se limiter à parler des images figuratives, de peintures, de films, etc. Il est évident que les images, leur production et leur conception font partie de la visibilité, mais beaucoup d'autres phénomènes viennent s'y greffer. Ne pouvant se réduire à sa simple dimension visuelle, l'auteur indique que la visibilité est « an impersonal, social field where subjects and sites of visibility play their role and contribute to determine effects in/of reciprocal visibility » (2007 : 339). Pour donner une certaine consistance à cette catégorie, l'auteur formule une série de caractéristiques propres à la visibilité. On peut donc, de façon provisionnelle, établir que la visibilité est « relational, strategic and processual or, better « eventual » » (Brighenti, 2010 : 25).

La visibilité est d'abord une affaire *relationnelle*. Elle suppose une relation entre voir et être vu. Cette relation est révélatrice d'une puissance qui ne se limite pas à l'objet de vision, mais est pleinement constitutive du sujet. Ce constat part principalement des travaux de Georg Simmel (1908) qui a étudié la fonction sociologique de l'œil. Simmel a identifié dans la fonction du regard sa capacité à instaurer un point de contact et une liaison entre les individus. Selon ce dernier, cette relation physionomique, dénuée de toutes formes médiatisées, constitue la base même de la sociabilité. Le fait que Simmel fasse de l'échange de regards l'une des formes les plus élémentaires de la sociabilité part du principe qu'elle permet « an understanding of the other which is not filtered by general categories but is instead truly individual and singular » (Brighenti, 2010 : 25).

Brighenti rappelle toutefois que l'échange du regard ne peut se concevoir sous un angle parfaitement symétrique. En ce sens, si les possibilités de vision suggèrent un fonctionnement biologique, elles instaurent également un ordre social en sélectionnant ce qui doit être vu et non vu (Foster, 1988). Cet effet d'asymétrie et de distorsion est d'ailleurs ce qui engendre la

question de la *stratégie*. Face à la vertu d'être source d'attention, la visibilité devient un acte stratégique ; et c'est cette dynamique manipulatoire qui permettra d'attirer l'attention sur le sujet ou le groupe voulant obtenir des effets sociaux (Brighenti, 2010 ; Voirol, 2005b).

Ces reliefs de l'asymétrie permettent de reconnaître les marges d'*incertitudes et d'éventualités* de la visibilité. Brighenti indique que la visibilité concerne toujours des sites, des sujets, des événements ou des rythmes qui donneront une consistance à ce qui sera vu. Il importe dès lors de ne pas adosser à la visibilité une linéarité a priori. La figure de la visibilité n'est pas donnée en soi, mais peut s'incarner en tant que dimension habilitante (reconnaissance) ou en tant que dimension assujettissante (contrôle). Considérer la visibilité c'est toujours lui reconnaître qu'elle peut conférer du pouvoir en même temps qu'elle peut en retirer. L'analyse de la visibilité n'est donc pas simplement une affaire de pure vision, mais une analyse de ses effets d'autonomisation et d'impuissance.

1.1.2. De la coprésence à la visibilité médiatisée

À travers la section précédente, on comprend que la visibilité ne peut se réduire à sa simple dimension visuelle, mais doit être appréhendée dans une « économie de l'attention » (Citton, 2014) plus globale. C'est ce que proposent d'étudier les travaux sur les médias de communication. Le terme de *média* qualifie habituellement le moyen de diffusion ou de communication pour transmettre de l'information (Proulx, 2015b). Dans l'ensemble, les *médias* renvoient à une série de supports matériels et de dispositifs socio-techniques :

> It is usually understood as including modern inventions such as the printed book, the press, photography, optical toys such as the magic lantern and other precinematic moving image systems, the cinema, the electronic media of radio and television and, finally, the fluctuating family of digital media known as the "new media". (Brighenti, 2010 : 71)

Les études sur les médias de communication ont habituellement appréhendé la question de la visibilité sous l'angle des supports symboliques et des médiations techniques capables d'étendre le « spectre de ce qui peut être vu » (Voirol, 2005b : 14). Walter Benjamin (1963) a notamment montré combien les nouvelles techniques de visualisation ont transformé les façons de percevoir. À propos de la photographie, l'auteur indiquait qu'elle a permis d'accroître démesurément le champ des réalités qu'ignore toute vision naturelle : « elle peut faire ressortir des aspects de l'original qui échappent à l'œil et ne sont saisissables que par un

objectif librement déplaçable pour obtenir divers angles de vue : grâce à des procédés comme l'agrandissement ou le ralenti » (p.275). En second lieu, par l'entremise de la technique, la reproduction est en mesure d'être transportée dans des situations où l'original lui-même ne pourrait se trouver. Sur le cinéma et la caméra, l'auteur souligne combien les appareillages techniques et les montages occupent un rôle majeur dans la performance de l'acteur qui se trouve maintenant soumis à une multitude de tests optiques.

Les travaux de Thompson (1995) ont permis d'approfondir la réflexion des changements liés au développement des médias de communication, des premiers écrits imprimés jusqu'aux réseaux électroniques. Pour l'auteur, il ne s'agit pas d'envisager l'utilisation des médias de communication comme de simples outils de diffusion d'informations qui laisseraient la relation intacte, mais de souligner combien leur développement a changé la nature des interactions humaines : « le développement des médias crée de nouveaux champs d'action et d'interaction qui impliquent des formes distinctes de visibilité et dans lesquelles les relations de pouvoir peuvent se déplacer rapidement, fortement et de manière imprévisible » (Thompson, 2005 : 66).

Avant l'arrivée des médias de communication, l'auteur nous explique que notre expérience et connaissance du monde reposaient sur l'instantanéité et la réciprocité, elles se structuraient dans *l'ici et maintenant*. Nos interactions étaient quant à elles régies à partir d'un cadre spatio-temporel commun et des relations de face à face. Alors que dans ce type d'interaction, les participants sont instantanément visibles l'un pour l'autre, l'avènement des médias de communication a permis de dépasser les frontières temporelles et spatiales spécifiques à l'interaction située. Il ne s'agit pas d'entrevoir les interactions médiatisées comme étant venues remplacer les interactions face à face, mais plutôt comme un complément à ces dernières. Comme nous venons de le souligner, l'une des spécificités des médias de communication est de libérer la visibilité des propriétés de coprésence, lui octroyant dès lors un nouveau départ. Cette nouvelle dimension intrinsèque à la visibilité médiatisée permet d'étendre notre champ du visuel dans l'espace et le temps, offrant une série de nouvelles possibilités :

> On peut être témoin, en direct, d'événements se produisant dans les lieux éloignés, c'est-à-dire au moment même où ils se déroulent en temps réel ; on peut également être témoin d'événements éloignés qui se sont produits dans le passé et qui, grâce aux qualités de préservation du médium, peuvent être représentés dans

> le présent (…). Des personnes peuvent être vues par beaucoup de spectateurs sans qu'elles ne puissent elles-mêmes les voir, alors que ceux qui regardent peuvent voir d'autres personnes éloignées sans être vus par elles. (Thompson, 2005 : 66).

Tout semble indiquer que l'accroissement des relations médiatisées a permis un nouvel espace d'apparence qui a élargi le sens de l'horizon de la visibilité et de l'expérience (Voirol, 2005b). Les médias de communication deviennent les principaux dispositifs qui permettent de créer et de maintenir un espace d'apparence ; et donc, les principaux canaux par lesquels les acteurs peuvent se rendre saisissables les uns aux autres et faire apparaître publiquement leurs actions et leurs paroles. L'auteur constate ainsi qu'ils ont contribué à générer une forme nouvelle de la scène du visible qui est non localisée spatialement et contient une pluralité d'acteurs qui ne sont pas obligatoirement présents sur le lieu de leur articulation.

En raison de cette nouvelle logique, la visibilité médiatisée présente l'avantage d'être accessible à un ensemble d'acteurs isolés qui permet l'expérience d'un *voir ensemble* (Voirol, 2005b). La construction de ce regard commun ne signifie néanmoins pas forcément que tous voient la même chose. Au contraire, le voir est intrinsèquement dépendant de l'horizon d'attente de chacun ; tous ne sont pas toujours d'accord sur ce qui est vu et sur ce qui mérite une attention. Le visible reste soumis au jugement de sujets qui s'inscrivent dans un langage et des actions et qui sont en mesure de remettre en question ce qui doit être vu.

Ces transformations auront plusieurs conséquences. Premièrement, pour Thompson (1995), la visibilité médiatisée est maintenant liée aux propriétés spécifiques des médias de communication, à savoir les dimensions socio-techniques du dispositif de diffusion avec le mode de circulation correspondant (manuscrit, imprimerie, numérique). Avant de s'interroger sur les dimensions personnelles, culturelles ou institutionnelles qui poussent un individu ou un groupe à une exposition médiatique, il faut s'interroger sur les moyens techniques qui les fabriquent (Heinich, 2012). Cela rejoint dans une certaine mesure la perspective médiologique du philosophe Régis Debray (1991) qui adopte un point de vue matérialiste. Selon ce dernier, bien que le support soit ce qui se voit le moins, il est ce qui compte le plus. À ses yeux, le matériau conditionne l'outil d'inscription, qui lui-même suggère la forme d'écriture.

Outre ces soubassements matériels et techniques des dispositifs de diffusion, une troisième conséquence tient au fait que les relais institutionnels et le dispositif des écrans ont entraîné

une redistribution des relations de pouvoir entre le visible et l'invisible (Mondzain, 2002). Avec l'avènement de la télévision et d'internet, les écrans sont devenus le lieu privilégié d'apparition d'images. La spécificité de l'écran est qu'elle occupe une double fonction (Barus-Michelle, 2011). La première est de s'interposer (faire écran) entre une réalité et celui qui la regarde. La seconde est de lui exposer une réalité en image. La réalité en image ne donne cependant pas d'indications sur le fait qu'elle soit imaginaire ou réalité. Effectivement, elle peut faire l'objet de modifications, de déformations, de trucages, d'effets spéciaux qui résultent d'un auteur dissimulé, de ses intentions, opinions et émotions, mais aussi de la technique, de l'angle de prise de vue, du montage ou des circonstances.

Pour l'auteur, « le visible est ce qui est perçu par les sens qui ne garantissent cependant rien de la réalité » (p.26). L'écran est donc à la fois un espace réel et le lieu de la fiction (Mondzain, 2002). Dans ce contexte où la visibilité médiatisée rend compte d'une portion du monde qui est perçue par un médiateur, qui s'objective dans des supports et qui est observée par un sujet à partir de son regard propre et son univers moral-pratique, toute visibilité fait l'objet d'une attention sélective qui opère sur le mode du découpage (Voirol, 2005b). Ainsi, les technologies de communication ne sont pas neutres et instaurent une hiérarchie dans la visibilité. Cela fera naître, ce que Voirol (2005b) nomme des luttes pour la visibilité.

Ces travaux sur la visibilité médiatisée ont le mérite d'avoir soulevé deux points majeurs. Premièrement, ces études souscrivent à dépasser une vision instrumentaliste des techniques, en donnant aux médias de communication un contenu substantiel. Ensuite, ils ont émis une analyse fine de l'évolution des technologies de communication et ce qu'elles permettent sur le plan de la vision. Si ces études ont raison de défendre l'idée que ces technologies ne sont pas neutres, elles semblent adhérer a priori à une épistémologie déterministe en les réifiant comme un supplément matérialisé de la vision humaine dont ses effets seraient plus efficaces. Or, en prenant la technique comme allant de soi, ces études excluent le fait que la visibilité médiatisée est le fruit d'une longue chaîne de médiation qui lui donne sa consistance et son contenu.

Elles rationalisent ainsi l'idée qu'un simple changement dans les technologies de communication produirait une incroyable transformation dans le contenu de la visibilité lui-même. Ces études renforcent une tradition importante dans les études en communication qui, à partir des caractéristiques des technologies de communication, ont considéré le médium

comme une extension de la perception sensorielle humaine et de l'action communicative dans le temps et l'espace (Carey, 1989 ; Ong, 1982 ; Williams, 1981). Cette perspective a pour le mieux été incarnée par McLuhan (1964) qui a défini le médium comme une extension de l'homme, de son corps aussi bien que de son esprit.

1.2. Mouvements sociaux et visibilité

Maintenant que nous en savons plus sur la visibilité médiatisée, nous nous intéresserons désormais à la relation entre la visibilité, les médias et les mouvements activistes. Pourquoi la visibilité constitue-t-elle une ressource essentielle pour les mouvements sociaux ? Comment la visibilité des groupes protestataires s'est transformée au cours du temps ? Ce sont à ces questions que tentera de répondre cette section. Pour les remettre en contexte, commençons par faire une brève revue de la littérature sur la sociologie des mouvements sociaux.

1.2.1. Sociologie des mouvements sociaux

Les mouvements sociaux se définissent souvent comme des « formes d'action collective concertée en faveur d'une cause » (Neveu, 2015 : 9). Les mouvements sociaux, et plus généralement l'action collective, ont fait l'objet d'une littérature abondante. Ce domaine de recherche a connu un fort développement depuis la fin des années soixante-dix aux États-Unis et en Europe. C'est particulièrement aux États-Unis que se sont établis la plupart des modèles théoriques : celui de la mobilisation des ressources, puis ceux de processus politique et des cadres de l'action collective (Mathieu, 2004). Ces travaux ne sont toutefois par restés sans critiques. De nombreuses zones d'ombres ont été évoquées, notamment en ce qui concerne le rôle des émotions dans l'action collective. Devant l'étendue des travaux sur les mouvements sociaux, il vaut sans doute la peine d'esquisser un premier balisage et d'examiner les différentes facettes de la question. Il s'agira dans ce qui suit de s'arrêter, un instant, sur les perspectives les plus courantes, sans toutefois, prétendre parvenir ici à faire le tour de la question.

La mobilisation des ressources

Dans les années 1970, l'étude sur les mouvements sociaux allait connaître un renouvellement décisif avec l'apparition d'un nouveau cadre d'analyse : celui de la mobilisation des ressources. Ce courant s'est établi entre autres en opposition aux théories du *comportement*

collectif. La validité des explications de l'action collective par l'anomie, l'irritation ou le degré de frustration était remise en cause (Gamson, 1975). L'intérêt pour les formes d'action collective ne consistait plus à se demander *pourquoi* des groupes se mobilisent, mais *comment* se cristallisent des mobilisations (Neveu, 2015). Au sein de la littérature sur la mobilisation des ressources, deux grandes tendances peuvent être identifiées (Perrow, 1979) : ceux qui adoptent une logique explicative de type économique, sous l'influence d'Olson (Mac Carthy et Zald, 1973), et ceux qui prennent en compte les variables historiques et sociologiques (Gamson, 1975 ; Obershall, 1973 ; Tilly, 1978). Malgré les différences qui existent entre ces théories, toutes partagent le même paradigme utilitariste de la rationalité individuelle (Fillieule et Péchu, 1993).

Voyons brièvement ces trois variantes principales. Mac Carthy et Zald (1973, 1977) s'inscrivent dans l'approche économique d'Olson. Ils fondent l'idée que les mouvements sociaux sont des « structures de préférences dirigées vers le changement social » (Mac Carthy et Zald, 1973 : 251). Dans cette perspective, ces derniers sont tributaires de *social movement organisations* (SMO). Les SMO fonctionnent comme des instances stratégiques, c'est-à-dire qu'elles identifient des buts et assemblent les ressources nécessaires. Comme pour les entreprises, les SMO reposent sur des principes d'offre et de demande. Dans les cas où des SMO sont dirigées vers un but commun, un *social mouvement industry* (SMI) émergera. Les SMI pourront quant à elles réunies au sein de *social mouvment sectors* (SMS). Tel que l'attestent les auteurs, il existe différents types de soutien au sein des organisations : les adhérents et les membres actifs (*constituants*). La première catégorie concerne les personnes et les organisations qui soutiennent le mouvement, mais qui ne disposent pas de ressources. La seconde catégorie renvoie aux personnes qui apportent des ressources aux mouvements (argent et temps). Pour Mac Carthy et Zald « les groupes les plus susceptibles de se mobiliser en raison de leurs attentes ne sont pas forcément les plus actifs dans la mesure où le succès ne dépend pas essentiellement du nombre ni de la volonté des personnes directement concernées » (Fillieule et Péchu, 1993 : 84).

Dans son livre *Social Conflicts and Social Movement* publié en 1973, Obershall indique vouloir étendre la théorie d'Olson, en proposant une dimension sociologique. Tout comme Olson, Obsershall considère l'organisation comme une condition sine qua non à l'action collective. Pour Obershall, la réussite d'un mouvement est liée à un ensemble de ressources. Elles peuvent concerner l'étendue du groupe (nombre de membres, intensité des liens, etc.), le

sentiment identitaire (la force du nous) ou encore des capacités stratégiques (possibilités de perturbations du groupe, capacité de diffuser des discours recevables, connexions à des centres de pouvoir, etc.).

Mais, c'est à Tilly (1978, 1986) que l'ont doit l'une des formes les plus abouties de la première génération des travaux de la mobilisation des ressources. L'originalité de Tilly est d'avoir pris en compte la sociabilité, les stratégies et la politique des mobilisations, en situant sa réflexion dans le temps long. Le fait d'opter pour une approche historique et comparative, lui a permis de saisir les évolutions de l'action collective qui se sont produites dans les pays européens et aux États-Unis entre le 16e et le 20e siècle. Il montre notamment comment des évolutions structurelles affectent les répertoires d'action collective et comment ceux-ci évoluent au cours du temps. Tilly définit le répertoire d'action collective comme « une série limitée de routines qui sont apprises, partagées et exécutées à travers un processus de choix relativement délibéré » (1995 : 26). Ce concept suggère ainsi qu'il existe des modes d'action institutionnalisés par les mouvements sociaux.

L'influence du contexte politique

Un autre apport important de Tilly (1978) est d'avoir pris en compte le contexte politique pour expliquer les mobilisations. L'auteur a porté son intérêt sur les différentes associations entre les gouvernements, les autres membres de la *polity* et les participants. Tilly met en relief l'importance pour les mouvements sociaux d'avoir accès aux autorités publiques, ainsi que les affrontements pour l'accès aux ressources politiques. La prise en compte du rapport entre l'action collective et le système politique a été poursuivie et élargie dans les années 1980 par, entre autres, Doug McAdam (1982) et Sidney Tarrow (1989). Dans son ouvrage sur le mouvement noir aux États-Unis, McAdam a notamment emprunté le concept de « structure des opportunités politiques »[7] pour expliquer l'émergence du mouvement des droits civiques aux États-Unis dans les années 1950 et 1960. Poursuivant le modèle du processus politique de Tilly, McAdam soutient ardemment que le développement d'une mobilisation dépend de l'environnement politique. Effectivement, pour l'auteur, en fonction de l'ouverture ou la fermeture du système politique, les ressources d'un mouvement militant pourront être

[7] Cette notion est apparue dans les années 1970, lorsque Peter Eisinger (1973) a étudié l'apparition des mouvements Noirs dans une cinquantaine de villes américaines. Selon l'auteur, le développement d'un mouvement social est fortement lié aux conjonctures du système politique (c'est-à-dire, les ouvertures, les fermetures, les restrictions ou encore les ressources).

mobilisées ou non. L'auteur précise toutefois que la structure des opportunités politiques n'est jamais définie a priori, elle évolue au gré d'événements sociaux, pouvant ainsi mener à des changements dans les opportunités politiques.

À ce stade, ce qui est entendu par conjoncture politique reste vague. C'est ainsi que des auteurs ont tenté de circonscrire les structures d'opportunités politiques. Tarrow (1984) a notamment identifié quatre dimensions clés : l'ouverture ou la fermeture du système politique ; la stabilité ou l'instabilité des alliances politiques ; l'accès à des positions stratégiques et les conflits entre élites ; les stratégies de politiques publiques et leur élaboration. Ces développements théoriques présentés sous une forme condensée nous permettent pourtant de souligner l'influence primordiale de l'environnement politique dans le passage à l'action collective. Disposer de ressources ne suffit donc pas à expliquer l'émergence d'un mouvement social.

Les cadres de l'action collective

Au tournant des années 1980, un ensemble de travaux menés aux États-Unis ont remis en cause le courant de la mobilisation des ressources. Plus particulièrement, ces travaux ont amorcé un tournant cognitif dans l'étude de la sociologie des mobilisations, jusque-là centrée sur la disponibilité des ressources, la création d'opportunités ou encore le calcul coût-bénéfice (Contamin, 2010). Il était cette fois-ci question de considérer l'importance de la mise en sens pour mobiliser ou contre-mobiliser une action collective (Benford et Snow, 2012). Cet intérêt pour le travail de la signification au sein des mouvements sociaux a contribué à raviver les dimensions subjectives, symboliques et culturelles, longtemps absentes de la théorie de la mobilisation des ressources (Mathieu, 2002).

En ce qui concerne les actions collectives, la perspective des cadres (*frames*) a largement été mobilisée pour rendre compte des composantes cognitives et discursives de l'action collective (Benford, 1997 ; Benford et Snow, 2000 ; Gamson, 1992 ; Snow et al., 1984 ; Snow et Benford, 1988, 1992 ; Tarrow, 1994)[8]. S'inspirant de la perspective goffmanienne des cadres, Snow et ses collaborateurs (1986) ont appliqué le concept de cadre à l'étude de l'action

[8] Contamin (2010) rappelle que plusieurs conceptions ont émergé pour développer la dimension symbolique et cognitive des mouvements sociaux (voir Turner, 1969 ; Piven et Cloward, 1979 ; McAdam, 1982). C'est toutefois la perspective des cadres qui s'est largement démarquée de ce champ de recherche, donnant lieu à de nombreuses publications.

collective. Cette perspective tranche avec la conception traditionnelle de l'idéologie, qui envisage les mouvements sociaux comme porteurs de croyances et de significations préexistantes. Elle soutient au contraire la nature active des mouvements sociaux dans leur faculté à construire, à maintenir et à reconfigurer le sens auprès de leurs partisans, leurs adversaires ou encore d'un auditoire extérieur (c'est-à-dire les médias, les autorités locales, l'État) (Snow, 2001 ; Snow et Benford, 1988). Effectivement, pour les auteurs, les mouvements sociaux « frame, or assign meaning to and interpret, relevant events and conditions in ways that are intended to mobilize potential adherents and constituents, to garner bystander support, and to demobilize antagonists » (Snow et Benford, 1988 : 198).

Par ailleurs, Snow et ses collaborateurs (1986) ont développé la notion d'alignement des cadres produits par des *leaders* pour signifier « the linkage of individual and SMO [social movement organizations] interpretive orientations, such that some set of individual interests, values and beliefs and SMO activities, goals, and ideology are congruent and complementary » (p.464). Les auteurs ont identifié quatre types d'opérations sous-jacentes à l'alignement des cadres. La connexion des cadres (*frame bridging*) forme l'opération la plus simple. Elle consiste à rapprocher deux ou plusieurs perceptions préexistantes, qui malgré leur congruence ne sont pas encore connectées. L'amplification de cadre (*frame amplification*) vérifie et clarifie les schémas interprétatifs existants, en insistant sur des croyances et valeurs résiduelles. L'extension de cadre (*frame extension*) s'inscrit dans une logique d'élargissement du cadre de l'organisation, en y intégrant des éléments présumés importants pour leurs potentiels partisans. La transformation de cadre (*frame transformation*) prévoit de modifier ou encore créer de nouvelles significations, de manière à ce que les opinions, les valeurs ou encore les croyances des individus concordent avec celles de l'organisation.

En étendant leur modèle en 1988, Snow et Benford relativisent le pouvoir d'alignement des cadres dans leur capacité à provoquer une mobilisation tangible. Selon les auteurs, un ensemble de conditions affectent ou limitent la production de cadres en vue de mobiliser de potentiels adhérents. Plus précisément, le cadre de l'organisation doit impérativement entrer en résonnance (*frame resonance*) avec les cibles de la mobilisation. Les auteurs proposent une trilogie pour rendre compte de la crédibilité et robustesse des cadres proposés par l'organisation : le cadrage de diagnostic (*diagnostic framing*), le cadrage de pronostic (*pronostic framing*) et le cadrage motivationnel (*motivational framing*).

Un levier supplémentaire à la perspective des cadres est ce que Snow et Benford (1992) nomment des cadres cardinaux (*master frames*)[9]. Pour Snow et Benford (1992), la fonction d'un cadre cardinal diffère peu d'un cadre d'action collective spécifique à un mouvement social. Ce qui change, c'est l'échelle et la portée du cadre. Les cadres cardinaux ont une portée de diffusion qui dépasse son foyer d'origine. Les cadres cardinaux ponctuent, articulent, attribuent, tout en étant susceptible de teinter et contraindre les cadres d'action collective d'autres mouvements sociaux. En cela, « master frames are generic ; specific collective action frames are derivative» (Snow et Benford, 1992 : 138). Enfin, notons que cette perspective invite à suivre les conflits subséquents au déploiement des cadres de l'action collective. Les cadres des mouvements sociaux sont soumis à de multiples confrontations et défis (Benford, 1993 ; Benford et Snow, 2012). Ceux-ci peuvent se regrouper sous trois grandes formes : « le contre-cadrage des opposants au mouvement, des auditoires et des médias ; les disputes sur les cadres au sein des mouvements ; et la dialectique entre cadres et événements » (Benford et Snow, 2012 : 242).

Certaines critiques ont été émises concernant la perspective des cadres de l'action collective. Particulièrement, une certaine réticence à la complexité des mouvements sociaux semble opérer au sein de cette perspective. Pour Mathieu (2002), le rôle des idées et des valeurs promues par une organisation n'est pas aussi déterminant que ne le prétendent les auteurs. Plutôt, la construction d'un mouvement protestataire est l'accomplissement d'intérêts et de motivations éparses et évolutives[10]. Selon Mathieu (2002), rien ne prouve que l'alignement des cadres et l'homogénéité de représentations ne puissent être considérés comme le mobile premier de l'engagement d'individus à un mouvement social.

Mathieu (2002) critique aussi les préjugés idéalistes du citoyen éclairé qu'on retrouve dans la théorie des cadres de l'action collective. L'auteur rappelle combien la sympathie pour un parti politique, voire son adhésion formelle, ne peut se restreindre à un nécessaire partage des représentations et à une pleine maîtrise de ses idéologies et concepts. Cette teinte

[9] Parmi les cadres de l'action collective susceptibles de fonctionner comme des cadres cardinaux, Benford et Snow (2012) listent, sans prétendre à l'exhaustivité, le cadre des droits, le cadre de l'autonomie du choix, le cadre d'injustice, le cadre de la justice environnementale, le cadre de l'opposition, la cadre du pluralisme culturel, le cadre du terrorisme sexuel, le cadre oppositionnel, le cadre de l'hégémonie et le cadre du « retour à la démocratie ».

[10] Par exemple, dans son ouvrage *Mobilisations de prostituées* (2001), l'auteur montre que les revendications sont doublement caractérisées. Alors que les travailleuses du sexe réclamaient le respect de leur activité et la non-stigmatisation, leurs soutiens chrétiens ou féministes renvoyaient la revendication de celles-ci à une « prise de conscience » du pouvoir aliénant de la prostitution.

d'intellectualisme dans la capacité mobilisatrice d'un collectif est pour l'auteur, à relativiser. L'impulsion d'une vision du monde partagée en accord avec les positions officielles, l'impérieuse injonction d'un alignement des cadres en amont de toutes mobilisations, est selon l'auteur, pour le moins discutable. C'est-à-dire, qu'en situation de mobilisation, il y a peu de raisons que celle-ci ne fasse pas l'objet de dissonance cognitive ou de déséquilibres dans les compétences politiques (Mathieu, 2002). De plus, la perspective des cadres insiste à maintes reprises sur la nécessité de la cohérence, de la complétude et du raffinement des discours organisationnels. Or, l'auteur objecte qu'à nouveau, rien ne permet de certifier qu'un discours très bien élaboré et sophistiqué puisse augmenter les chances de réussite d'une mobilisation. Sur cet aspect, l'auteur se demande si, a contrario, les discours ambigus et flous ne sont pas porteurs d'une plus grande résonnance, en raison de leurs capacités à adjoindre une multitude d'interprétations et d'appropriations.

La place des émotions

Au sein de la littérature sur les mouvements sociaux, le rôle des émotions a largement été négligé (Sommier, 2010). Cette réticence à reconnaître cette part de l'action collective s'explique entre autres par le rejet de théories psychologisantes et de l'étude de la psychologie des foules. Le fétichisme de la rationalité, propre à la mobilisation des ressources, a court-circuité toute dimension émotionnelle sous-jacente aux entreprises contestataires (Traïni, 2009). Toutefois, le renouvellement des émotions dans le paysage de la recherche sur l'action collective s'est renforcé à partir des années 1990 (Aminzade et MacAdam, 2001 ; Goodwin et al., 2001 ; Groves, 2001 ; Petersen, 2002 ; Taylor, 1995). Mais, cette réhabilitation des émotions s'est trop souvent imposée dans un registre instrumental et de manipulation des apparences (Cefaï, 2016 ; Sommier, 2009). En ce sens, les émotions ont été perçues comme étant stratégiquement mobilisées par les militants pour signaler la cause à d'autres adhérents et au monde extérieur (Goodwin et al., 2004). C'est notamment le cas de mouvements qui utilisent le répertoire des émotions pour modifier l'état émotionnel du public cible, comme dans le cas du terrorisme par exemple.

Plutôt que de voir les émotions comme instrumentalisant les sentiments des autres, certains auteurs ont envisagé la manière dont les émotions transforment la mobilisation (Cefaï, 2016). Les émotions deviennent un vecteur important qui relie sensibilité et engagements réflexifs (Neveu, 2015). Il n'est donc pas question de coût-bénéfice, mais de membres affectés par des

émotions (Cefaï, 2016 ; Gamson et al., 1982 ; Goodwin et al., 2001). Toute mobilisation est ponctuée par de l'indignation morale, de l'effroi, de l'enthousiasme, de la désolation, de la peur, de la surprise, de la colère ou du dégoût (Goodwin et al., 2004). Ainsi, les émotions ont une dimension constitutive de bien des moments de la mobilisation (Goodwin et al., 2001). Elles permettent d'unir ses membres en consolidant une communauté émotionnelle, qui provoque des émotions partagées, suscite des réactions coordonnées ou encore génère des élans affectifs (Della Porta, 1995 ; Jasper, 1998 ; Sommier, 2009). Avant de s'engager dans des stratégies, les adhérents sont donc d'abord affectés par une situation (Cefaï, 2016 ; Sommier, 2009).

Plusieurs manières de saisir de l'objet émotions ont fait surface dans le but d'analyser leur rôle dans l'engagement des mobilisations. Jasper (1997) a par exemple envisagé le *choc moral* comme l'une des caractéristiques les plus effectives pour consolider une action collective. La lecture qu'il fait des émotions est processuelle. Cela commence avec un événement imprévu qui implique des réactions physiques (écœurement, nausée, peur, dégoût, etc.) ; conduisant les personnes à jauger les conflits de valeurs ; impliquant une réaction immédiate qui l'amène à s'engager. Traïni (2008) soutient quant à lui que le moment de l'engagement dépend de « dispositifs de sensibilisation » déployés par des entrepreneurs de cause. Les dispositifs de sensibilisation se traduisent dans « l'ensemble des supports matériels, des agencements d'objets, des mises en scène, que les militants déploient afin de susciter des réactions affectives qui prédisposent ceux qui les éprouvent à s'engager ou à soutenir la cause défendue » (Traïni et Siméant, 2009 : 13).

Enfin, Sommier (2015) souligne pour sa part l'engagement à haut risque, qui se traduit dans des formes d'engagement plus radicales. L'engagement à haut risque a pour particularité d'être doublement affecté, en raison de l'effet qu'il produit sur la société, mais aussi sur l'individu engagé. Adopter ce type d'action peut être éprouvant pour le militant. Il doit généralement se couper de ses liens antérieurs, voir de son identité. Mais, ce type d'engagement nécessite aussi un fort contrôle émotionnel qui se veut à la fois collectif et individuel. Collectivement par le respect des règles de sentiments ou de sécurité, mais aussi dans certains cas, par l'exercice d'une violence extrême. Individuellement, « par les tensions affectuelles en raison de l'hypervigilance requise et les conflits intérieurs qu'il génère » (Sommier, 2015 : 5).

1.2.2. Rendre visible la contestation

Eu égard à ce qui précède, nous avons pu voir que les mouvements sociaux produisent des discours, parlent et mettent en place des « dispositifs de sensibilisation » (Traïni, 2008). Mais pour nécessaire que soit cette mise en mots, il faudra pour les militants rendre visible ce langage du mécontentement (Neveu, 2015). Pour cette raison, la visibilité a toujours constitué une ressource essentielle pour les mouvements contestataires, au point qu'elle peut être considérée comme un registre à part entière dans leur revendication (Bleil, 2005 ; Crettiez et Piazza, 2013a ; Voirol, 2005b). Pour qu'une action collective puisse exister, elle doit se rendre intelligible aux yeux des autres (Bleil, 2005). En ce sens, un groupe existe et agit une fois visible aux yeux des autres. La visibilité permet à un groupe de rendre sa contestation connue, autant pour les acteurs du groupe que pour des publics plus larges. C'est lorsque les militants atteignent la scène de la visibilité, que ceux-ci sont à même de mobiliser l'opinion publique, de susciter la réaction de leurs adversaires, de créer et maintenir une base de soutien, d'agir sur les politiques en vigueur et d'entretenir une relation indirecte avec les instances politiques instituées (Della Porta, 2010). Dès lors, pour Voirol (2005b), les luttes pour la visibilité ne peuvent s'étudier comme un aspect périphérique des mobilisations, elle doit au contraire être considérée comme une composante centrale. On proposera pour commencer de saisir ce que signifie d'apparaître publiquement, avant d'évoquer plus précisément le lien entre les technologies de communication et le militantisme.

Apparaître aux yeux des autres

Lorsqu'Hannah Arendt a approché en 1961 la question du domaine public et d'apparence au sein du public, elle a envisagé l'apparence comme le fait d'exister dans un monde commun partagé. Pour Arendt, apparaître dans le domaine public nécessite la consolidation de relations au sein d'un espace dont les référents sémantiques sont collectivement partagés. L'espace public qu'Arendt invite à penser, sans en utiliser le terme, s'inscrit dans le prolongement de la tradition hellénique et laisse au second plan la rhétorique du discours démocratique issu des

Lumières[11]. Dans son modèle, elle reprend le concept de la *polis*, qui selon sa terminologie, constitue l'espace d'apparence par excellence. Cet espace de dévoilement permet aux acteurs de se rendre visibles à un public de semblables, de se rencontrer et d'interagir. Ainsi, le domaine public réfère à une série d'apparences qui peuvent « être vues et entendues par tous et toutes et jouir de la plus grande publicité possible » (Arendt, 1961 : 89). Arendt postule que c'est par la *polis* que se déploie l'action, car l'action ne peut s'effectuer dans l'isolement. La *polis* est ce lieu qui constitue le sens de la réalité, qui permet la réciprocité et la création de l'identité de soi.

Une des particularités de l'analyse d'Arendt est qu'elle n'envisage pas l'espace public à partir de normes, mais qu'il s'agit avant tout d'un espace qui apparaît au gré des prises de parole. Plus précisément, l'espace d'apparence se bâtit dès que les individus se rassemblent dans le monde de la parole et de l'action. L'auteur apporte néanmoins une nuance. Elle explique que tout rassemblement dans le monde de la parole et de l'action ne fait preuve d'aucune constitution formelle du domaine public et des formes de gouvernement, à savoir les formes diverses au travers desquelles le domaine public peut s'établir. Par ce fait, l'espace d'apparence précède le domaine public.

Ainsi, au contraire d'Habermas qui a porté son attention sur la nature communicationnelle et à la raison pratique de l'espace public, en tant que phénoménologue, Arendt a accordé plus d'importance à la *scénarisation* (Quéré, 1992). L'auteur explique que le modèle du domaine public d'Arendt se fonde sur le modèle de l'esthétique et s'articule autour de trois principes majeurs : comme l'art, l'action de la politique se révèle à partir d'une scène d'apparition. Cette action politique est ensuite soumise aux « jugements réfléchissants » d'un public de spectateurs (dont le modèle chez Kant est celui d'un « jugement de goût » qui s'oppose au « jugement de connaissance ») afin de formuler à son égard des opinions prétendant à sa validité. Une fois ces opinions formulées, l'existence d'un monde commun pourra prendre naissance.

[11] Dans la tradition occidentale, il existe deux grands modèles de l'espace public : le modèle grec et le modèle bourgeois (Ferry, 1989). Ces deux grands modèles renvoient à différentes fonctions. Chez les modernes, dont leur perspective relève essentiellement de la conception habermasienne de l'espace public, ce dernier doit répondre à un impératif moral d'émancipation, tandis que chez les Grecs, l'espace public réfère à l'esthétique de la figuration, de la présentation de soi, où chaque individu doit pouvoir exceller pour parvenir à la gloire (Quéré, 1992).

Dans cette perspective, l'espace public est intimement lié à « un dispositif de configuration du collectif qui le rend visible et sensible à ceux qui y participent, d'un processus d'institution symbolique d'un espace d'appartenance et d'un monde commun, ou encore d'un mécanisme de création des conditions d'accès à liberté et à l'égalité » (Quéré, 1992 : 81). En appliquant un point de vue phénoménologique à la politique et à l'espace public, Arendt a mis l'accent sur le fait que ces champs ne doivent pas être considérés comme des objets, mais comme des *phénomènes* et des *apparitions*. Ils sont dès lors ce qui apparaît aux yeux et au sens et qui se manifeste d'emblée par eux-mêmes. Les phénomènes sont ainsi intrinsèquement dépendants de plusieurs composantes : ceux pour qui ils apparaissent, l'espace dans lequel ils surviennent et la relation qui existe entre les phénomènes et ceux qui les perçoivent.

Conflictualité

Jusqu'à présent, nous avons porté notre attention sur l'importance d'un monde commun basé sur des référents sémantiques collectivement partagés et sur la scénarisation de la vie sociale. Toutefois, Voirol (2005b) rappelle que pour Arendt, il est aussi un lieu où s'entrecroisent de manière dynamique des points de vue pluriels. Le monde commun n'est pas figé, il est renouvelé constamment et fait l'objet de « processus de déstructuration par la destruction des référents communément partagés » (Voirol, 2005b : 95). L'existence d'une multitude de points de vue et d'acteurs démontre la plasticité de l'arène publique, dans la mesure où « ses contours ne sont pas prédéterminés, mais varient à mesure que de nouveaux problèmes ou de nouveaux acteurs apparaissent et demandent à être pris en compte » (Macé, 2006 : 11). L'auteur apporte ainsi une précision importante à la dynamique de la sphère publique. La sphère publique n'apparaît pas seulement au gré des prises de paroles, mais se construit plutôt au fur et à mesure qu'une représentation ou un fait devient problématisé comme un problème d'ordre public par des acteurs.

Pour comprendre l'espace public, l'auteur stipule qu'il faut considérer ses dimensions conflictuelles, asymétriques, plurielles et plastiques. Ce dernier assume que l'espace public doit d'abord se comprendre comme un lieu de conflits de définitions, entre points de vue hégémoniques et contre-hégémoniques. Cela rejoint la définition de Wolton qui envisage « l'espace public comme un espace symbolique où s'opposent des discours contradictoires tenus par des acteurs (politiques, religieux, sociaux) qui composent la société » (cité par Serghini et Matuszak, 2009 : 32). L'organisation de la sphère d'apparence découle ainsi d'un

ensemble de luttes de légitimation et de disqualification au sein de rapports sociaux asymétriques. Macé (2006) précise toutefois que « cela ne signifie pas que la sphère publique soit nécessairement dominée par le point de vue des acteurs dominants, mais que les acteurs sociaux ou les points de vue subalternes dans les rapports sociaux asymétriques sont aussi subalternes dans la sphère publique et qu'ils doivent avant tout construire leur légitimité » (p.8). Ainsi, revenant à la perspective arendtienne, il peut être dit que chaque processus de publicisation politique répond à l'exigence de sens différentiels et d'intervalles de parole (Cefaï et Pasquier, 2003).

Problématisation

Dans cette dynamique de l'arène publique, la revendication, violente ou non, des mouvements sociaux se révèlera dans le cadre d'une scène d'apparence soumise aux jugements d'un ensemble de spectateurs. Comme nous l'avons vu avec Arendt, tout espace d'apparence peut exister potentiellement, mais pas nécessairement factuellement. Pour qu'un groupe atteigne la possibilité d'être vu et entendu par tous, cela nécessite de mettre en œuvre un registre expressif et une série de stratégies (Neveu, 2015). Cela rejoint la conviction de Cefaï (2016), selon laquelle une arène publique découle de la mise en mot d'une situation problématique.

Nous avons soulevé avec la perspective des cadres de l'action collective que les militants produisent des discours, des explications et des problématisations. Dans le monde des mouvements sociaux, cette dimension cognitive ne renvoie pas seulement à des croyances et des mythes mobilisateurs (Cefaï, 2016). Ce que les mouvements nous donnent à voir ce sont des récits et des arguments réflexifs. Ainsi, si les mots expriment des sentiments d'injustice, des partages d'expériences, des justifications, ils sont également porteurs de programmes et d'analyses théoriques (Neveu, 2015). C'est à partir de ce travail en profondeur qu'un mouvement sera en mesure de faire apparaître un problème à son public. Ce versant de l'activité militante engendre inévitablement une dimension normative (Cefaï, 2016 ; Neveu, 2015). L'avènement d'une problématisation confère aux militants le besoin de dénoncer des responsables, désigner des causes, formuler des explications, émettre des hypothèses et des résolutions.

Dès lors, pour que la problématique du mouvement fasse l'objet d'une reconnaissance (Honneth, 2005), les acteurs du groupe mettront en action une série de processus visant à

attirer l'attention du public (Bleil, 2005 ; Klandermans et Oegema, 1987). Ces processus sont à la fois individuels et collectifs : « chaque acteur se sent concerné par une manière de caractériser la situation et élabore un cadre commun d'action » (Bleil, 2005 : 128). Confronter leur action politique à un public, suscite d'une certaine façon des luttes de légitimation et de disqualification qui prendront forme au sein de cet espace. Ainsi, pour l'auteur, être visible n'est pas le produit d'un plan construit a priori, car la visibilité dépend d'actions qui s'élaborent à la suite d'événements et de décisions prises par différents acteurs. Les acteurs ne sont pas en mesure d'anticiper les enchaînements exacts de la mise en visibilité et sa portée publique réelle. À ce titre, l'auteur renvoie à la citation d'Albert O. Hirschmann pour qui « la société repose sur des "ratages", propose de ce fait de l'analyser en tenant compte des effets non intentionnels des actions humaines » (p.126).

1.2.3. Les transformations de la visibilité protestataire

Si les travaux qui précèdent nous ont permis d'entrevoir les dynamiques sous-jacentes à l'espace d'apparence et au domaine public, nous ne pourrions poursuivre plus avant sans prendre en compte l'émergence de puissantes institutions qui orientent les dynamiques d'apparence des militants. Il est un fait que l'arène d'expression des mouvements protestataires est inextricablement liée aux médias (Carroll et Hackett, 2006 ; Downing, 2008 ; Granjon, 2009 ; Neveu, 1999, 2010, 2015 ; Tarrow, 1994). Champagne (1991) disait à ce propos que les mouvements sociaux n'ont d'existence visible qu'à partir du moment où ils font l'objet d'un traitement médiatique. Sans image publique, les mouvements ne peuvent se faire connaître. Selon Gamson et Wolfsfeld (1993), les mouvements ont besoin des médias pour trois objectifs principaux : la mobilisation, la validation et l'élargissement du périmètre. Fillieu et Péchu (1994) considèrent ainsi que les médias sont pour les mouvements sociaux « un moyen institutionnel de réaliser des buts non intentionnels » (p.179). De surcroît, les technologies de communication s'avèrent être centrales pour gérer leur communication interne et externe. Fillieule et Péchu (1993) indiquent que la communication interne se restreint aux militants et aux adhérents et peut avoir des usages très divers. C'est-à-dire qu'elle peut porter sur l'organisation tactique et stratégique, mais aussi sur un travail de signification pour consolider et pérenniser l'engagement de ses membres. La communication externe s'adresse pour sa part aux adversaires potentiels, ainsi qu'au monde extérieur.

La multiplication des technologies de l'information et de la communication a engendré des changements incontestables pour les militants. Avant le développement des procédés de

l'imprimerie dans l'Europe du 15e et 16e siècle, la publicisation de contenus d'informations s'enracinait, pour la majorité des gens, dans des mécanismes de coprésence (Thompson, 2000). Nous avons déjà exposé dans la section sur la visibilité médiatisée que l'avènement de nouvelles technologies de communication a permis d'enregistrer des actions et d'élargir la portée de leur diffusion à des personnes qui n'étaient pas présentes sur le lieu au moment de son déroulement. Mais être visible par les médias, signifie d'être sous le joug des procédés d'amplification et de cadrage rhétorique des médias (Neveu, 2010).

Avec l'essor de l'imprimerie et des autres médias, les militants ont commencé à bénéficier de techniques de communication de masse pour partager leurs revendications. Entre 1517 et 1530, ce n'est pas moins de 300 000 exemplaires des trente écrits de Luther qui ont été vendus (Eisenstein et Mansuy, 1971). Au moment de la guerre civile en Angleterre, les presses londoniennes ont produit 4 038 titres en 1642 (un chiffre qui s'élevait à 848 en 1640) (Raymond, 2006). Parallèlement, une série de presses clandestines, qui ont pris racine dès 1640, ont largement opéré (Como, 2007). Sous la Révolution française, la presse qui avait toujours eu un rôle secondaire a connu une croissance exponentielle. Ainsi, l'imprimerie a rapidement joué un rôle majeur dans la propagande politique.

La circulation de tracts, livres, feuilles volantes, placards, caricatures, articles de presse s'est de plus en plus banalisée, permettant à des groupes clandestins et révolutionnaires de devenir visibles pour une grande frange de la population. Si ces mouvements s'emparaient des innovations de la presse, leurs images et récits étaient toutefois en compétition avec une presse populaire en pleine éclosion (Albert, 2010). Durant les deux premiers tiers du 19e siècle, la presse populaire a vécu une transformation profonde dans sa forme, son rythme et son ampleur. L'information devenait un produit de consommation banale et subit des transformations majeures dans sa forme. Il s'agissait de promouvoir une simplicité de style, des nouvelles divertissantes et des faits divers pour acquérir une plus grande audience. C'est ainsi que la presse anarchiste a par exemple dû se développer en marge d'une presse sensationnaliste à *un penny* (Bolt, 2012). Sachant qu'ils ne pourraient gagner la bataille de lectorat, les anarchistes ont plutôt misé sur le fait de contester les versions délivrées par la presse, que les lecteurs considéraient comme faisant autorité.

Cette autonomie médiatique s'est prolongée au sein de différents mouvements. Neveu (2010) donne l'exemple des mouvements communistes, social-démocratre-chrétiennes, qui jusqu'aux

années 1970 ont exploité un solide réseau de communication : quotidiens, revues, bulletins, feuilles volantes, tracts, affiches, livres (et parfois radio). Mais à ces formes de publicisation, s'ajoutent les médias dominants, qui restent un passage obligé pour assurer l'élargissement de la visibilité du groupe (Champagne, 1990, 1991 ; Gitlin, 1980 ; Granjon, 2009 ; Neveu, 1999, 2010, 2015). Par manque de ressources et de compétences, il n'est pas toujours possible pour les groupes de fabriquer un espace d'apparence alternatif (Granjon, 2009). Certes, si les médias dominants rendent visible le mouvement à une plus large audience, ils arrivent que ceux-ci imposent un cadrage du mouvement qui le disqualifie (Champagne, 1990 ; Gitlin, 1980 ; Granjon, 2009). Cette divergence entre l'image que le mouvement entend promouvoir et les représentations imposées par les médias fait naître ce que Gitlin (1980) appelle une « symbiose conflictuelle ». Nous verrons toutefois cette dynamique plus en détail dans la section 1.3.2.

L'avènement de nouvelles technologies de communication, telles que la radio et la télévision sont venues compléter ces « manifestations de papier » (Champagne, 1990). Si comme l'indique Thompson (2000), ces nouveaux médias s'inscrivent dans la continuité d'une visibilité médiatisée amorcée par des l'imprimerie, ils promeuvent aussi de nouvelles directions. Il est maintenant possible de diffuser la contestation dans un moindre délai et sur une plus grande distance (phénomène qui s'est considérablement amplifié avec l'arrivée de la télévision par satellite). Étant donné la teneur visuelle et auditive de ces technologies de communication, elles s'articulent à une grande variété d'indices symboliques. Il est donc maintenant possible d'apercevoir des traits spécifiques aux interactions face à face, même si elles divergent par leurs propriétés spatiales. La radio est en mesure de diffuser la voix, tandis que la télévision fait parvenir à des individus éloignés des indices oraux et visuels. La télévision a ceci de spécifique : faire de la publicisation un acte de plus en plus visuel, au sens de la vision.

Ces nouvelles formes de médiatisation ont ainsi participé à façonner l'espace d'apparence des mouvements sociaux. L'apparition de la radio a par exemple mené les groupes militants à parler directement à la population, en créant par exemple des *Radios Libres* (comme la radio *Lorraine Cœur d'acier* des sidérurgistes en 1978) (Fillieule et Péchu, 1993). Par ce média, les militants pouvaient faire entendre leurs voix et cadrer le sens de leur revendication (Filieule et Péchu, 1993), en permettant une forme particulière d'intimité (Thompson, 2000). L'auteur explique qu'avant l'apparition de la radio, l'art oratoire s'exerçait au sein de rassemblement à

petite ou grande portée. L'orateur se situait au-dessus de l'auditoire, utilisait souvent un langage enflammé et devait projeter sa voix avec force. Selon l'auteur, la radio a permis de réduire cette forme distante associée à la rhétorique, en faisant place à une sorte d'« intimité médiatisée » qui rendrait les interventions plus amicales.

La télévision a pour sa part causé une nouvelle forme d'intimité au sein de l'espace public. Partant de l'analyse des *leaders* politiques, l'auteur explique que le public est maintenant en mesure d'observer méticuleusement les énonciations, les émotions, l'apparence personnelle, les traits singuliers ou encore le langage corporel des dirigeants. Cette observation minutieuse peut aisément se transférer à des militants, puisque ceux-ci font un large usage de ce médium. Bolt (2012) explique à cet égard que la télévision est devenue une ressource essentielle pour les groupes insurrectionnels. C'est par la télévision qu'ils pourront propager leur spectacle et créer des moments de choc visuel pour faire les gros titres, attirer les projecteurs médiatiques ou encore déclencher le suivi en direct de leur action[12].

Ce type d'interaction médiatisée reste cependant confiné au statut de quasi-interaction, étant donné que le flux d'information reste majoritairement à sens unique (Thompson, 2000). Le lecteur d'un journal, l'auditeur ou encore le spectateur d'un programme télévisuel, « sont les destinataires d'une forme symbolique dont le producteur n'exige pas (et ne reçoit généralement pas) de réponse directe et immédiate » (Thompson, 2000 : 192). La convergence de l'informatique et des télécommunications dans les années 1980 a pour sa part changé le paysage médiatique des activistes. Alors que les technologies de communication présentées ci-dessus ont été de type *one-to-many*, internet permet une communication de type *many-to-many* (Bolt, 2012). Avec internet, les mouvements militants sont plus à même d'être autonomes dans leur communication, en créant et diffusant directement leur propre message (Cardon et Granjon, 2013 ; Neveu, 2010).

[12] Par exemple, lors du détournement du vol TWA 847 par des terroristes chiites du Hezbollah (agissant sous le nom de l'Organisation des opprimés de la terre) le 1er juin 1985, les médias ont largement couvert l'événement. La particularité de cet événement est qu'il a maintenu l'attention des médias dans un temps long en détenant une trentaine d'otages américains ont été détenus à bord de l'avion à Beyrouth pendant une durée de 17 jours. Durant cette période, 500 sujets d'information (28,8 par jour en moyenne) ont été enregistrés (Hoffman, 1999). Ils ont été diffusés par trois chaînes principales de télévision américaine : ABC, NBC et CBC. Les journaux télévisés consacraient en moyenne 14 minutes sur 21 à la crise. Pas moins de 80 flashs d'information et d'éditions spéciales ont interrompu les programmes en cours. Ainsi, tout en communiquant du sens, les insurgés ont cherché à créer un événement médiatique de grande ampleur (Bolt, 2012).

Toutes ces choses démontrent que les stratégies communicationnelles passent par différents moyens. Il y a les stratégies qui visent à contrôler le processus de production du contenu médiatique et celles qui cherchent à interpeller les journalistes. Ainsi, on a vu par exemple que dans des contextes historiques passés les mouvements sociaux ont manipulé d'importants réseaux de médias, alliant la radio, les revues, les bulletins, feuilles volantes, tracts, affichage de rue, etc. Bien que ces techniques se soient raréfiées, l'autonomie médiatique s'est toutefois réactualisée avec l'avènement d'internet (Neveu, 2010). La dépendance à l'égard des médias publics ou privés n'a pour sa part jamais déserté le paysage médiatique des militants (Granjon, 2009 ; Neveu, 2010).

Il importe de terminer en signalant que le contrôle de l'information est un enjeu de lutte entre l'État, les intermédiaires, les adversaires et les militants (Bolt, 2012). Par ce fait, les rapports entre médias et mouvements doivent être analysés comme un processus interactif (Fillieule et Péchu, 1993). Les pouvoirs en place peuvent institutionnaliser une série de mesures de surveillance, de censure et de contrôle des intermédiaires techniques (Tréguer, 2017)[13]. La censure peut être doublement effective, en s'effectuant a priori ou a posteriori. Les autorités publiques peuvent également contrôler assidûment les intermédiaires, en leur imposant des contraintes ou des poursuites. Ces archétypes du contrôle étatique ne sont pas les seules difficultés éprouvées par les militants. Les intermédiaires peuvent exercer un filtrage de l'information par des *gatekeepers* et modérer l'information (Cardon, 2010 ; Gillespie, 2018 ; Roberts, 2019). Être visible confronte aussi les militants à des contre-mouvements qui leur opposent des définitions de sens. Ils remettent alors en cause publiquement le cadre interprétatif du mouvement (Benford et Snow, 2012). Cela renvoie à ce qui peut être désigné de contre-cadrage. Il existe alors une confrontation de sens tenace entre les mouvements et les opposants. Pour résumer, les militants se heurtent à une lutte « pour l'accès à l'information et pour la définition du sens de l'action » (Fillieule et Péchu, 1993 : 189). La visibilité d'une action collective rivalise donc avec une myriade d'acteurs qui ont leurs propres logiques (Bolt, 2012).

[13] À titre d'exemple, le 19 octobre 1988, le Secrétaire de l'intérieur Douglas Hurd avait annoncé que le gouvernement conservateur interdirait à la radio et à la télévision britannique de diffuser des entretiens avec les groupes paramilitaires républicains du nord de l'Irlande. Cette interdiction s'est également étendue aux représentants du *Sinn Fein*, l'aile politique de l'IRA, qui détenait un siège au Parlement. La justification de Hurd était que « the terrorists draw support and sustenance from their exposure in the news media. The gouvernement has decided that the time has come to deny this easy plateform to those who use it to propagate terrorism » (cité par Sleuter, 1990 : 258).

1.3. Activisme extrémiste et visibilité

Des termes comme terrorisme ou extrémisme peuvent se révéler inconsistants dans le travail d'analyse (Sorel, 2002 ; Sotlar, 2004). Ils renvoient à des catégories peu stables, qui constituent un terrain de dispute en raison de leur imprécision sur le plan juridique, philosophique, sociologique et psychologique. Ils dénotent une dimension normative en ce qu'ils sont généralement considérés comme représentant les tendances idéologiques les plus éloignées du spectre politique conventionnel (Backes, 2004 ; Sotlar, 2004). Plus que des concepts scientifiques précis, ils appartiennent davantage au lexique politique, qui n'existe que dans un contexte culturel et historique particulier (Backes, 2004 ; Chaliand et Blind, 2015). De la fin du 19e siècle jusqu'à la seconde moitié du 20e siècle, le terrorisme était l'affaire des anarchistes, nihilistes, populistes, racistes, marxistes, fascistes et des nationalistes. Au tournant du 20e siècle, le terrorisme religieux est réapparu avec l'islam radical.

Ainsi, entre les groupes bien définis qui cherchent à obtenir l'indépendance d'un État, une autonomie ou une reconnaissance, et ceux aux contours plus vagues qui se fondent à partir d'un combat de civilisations (opposition religieuse, culturelle ou de puissance), l'idée d'une définition objective devient ardue (Sorel, 2002). Le sens commun du terrorisme contemporain se comprend habituellement comme étant « des actes de violence exécutés par des groupes politiques généralement clandestins, dans la volonté de créer un climat d'insécurité, d'affaiblir un régime, de désorganiser un système d'oppression visant tant les individus que les biens » (Sorel, 2002 : 37). Si parler d'extrémisme ou de terrorisme relève plus d'un discrédit que d'un type d'activité particulier, il est préférable d'envisager le terrorisme comme un mode de lutte (Merari, 2015). L'aborder sous ce point, témoigne d'une récusation d'un point de vue moral, au profit d'une démarche qui permet de distinguer les diverses conditions et formes de la violence politique.

Il est un fait qu'au sein de certaines formes extrêmes des champs politiques, le langage de mécontentement s'accompagne de formes radicales de violences (Crettiez, 2010). L'auteur dira à ce propos que l'acte de la violence politique vise à « faire exister une parole dans l'espace public, à briser une marginalisation ressentie, à confronter un point de vue, à négocier des avantages ou à détruire des pouvoirs ou des représentations » (p.9). Une violence qui peut aussi se traduire dans des formes iconoclastes et devenir la signature d'un acte terroriste, comme les attentats du 11 septembre 2001. Ainsi, la violence politique

communique et cherche à se rendre visible. Nous verrons dans ce qui suit les différentes stratégies de communication déployées par des militants qualifiés de terroristes. Dans un second temps, nous verrons comment ces groupes acquièrent la visibilité à travers les médias traditionnels et les nouveaux médias. Nous nous questionnerons pour terminer s'il existe une différence nette entre les différents médias dans l'écosystème médiatique des activistes.

1.3.1. Stratégies de communication

Toute communication politique repose sur deux piliers : la définition et la répétition (Bolt, 2012 ; Domenach, 1973). Des dimensions que les groupes insurrectionnels ont profondément intégrées. Ils savent qu'ils devront répéter et transmettre inlassablement leurs messages dans l'espace public pour familiariser le public à leur cause. Au sein de la littérature, il est courant d'envisager la communication comme étant un axe central du terrorisme (Chalfont et al. 1980 ; Fischer et al., 2010 ; Schmid et Graff, 1982 ; Tuman, 2009). Comme le soutiennent Schmid et Graff (1982), « terrorism can be understood as a violent communication stratgy. There is the sender, the theorist, a message generator, the victim, and a receiver, the enemy and/or the public » (p.45).

Le recours à la communication assure un rôle primordial pour attirer l'attention, et par conséquent assurer la survie et la longévité du groupe (Matusitz, 2013). Il existe donc de multiples finalités à la communication de groupes insurrectionnels : transmettre un message et créer un climat de peur auprès des groupes cibles ; mobiliser un soutien plus large en évoquant des thèmes tels que l'importance de leur cause et leur inéluctable victoire ; perturber les réponses des autorités publiques en discréditant les mesures anti-terroristes en vigueur ; accroître le recrutement en incitant de potentielles recrues à rejoindre le mouvement (Wilkinson, 1997). Sans communication, il est donc fort probable que les mouvements qualifiés de terroristes peinent à recruter de nouveaux adhérents et à motiver leurs membres.

Qu'il s'agisse des anarchistes révolutionnaires du 19^{e} siècle, de l'Armée républicaine irlandaise, des Brigades rouges, d'Al-Qaïda, de groupes d'extrême droite, tous emploient des stratégies de communication. Mais, selon les époques, ces groupes n'ont pas bénéficié de méthodes de communication similaires. Effectivement, les innovations en matière de moyens de communication se sont avérées être primordiales pour la visibilité d'auteurs d'actes terroristes. À ce titre, Bolt (2012) explique que le principal échec des anarchistes du 19^{e} siècle

est dû, entre autres, à leur incapacité de contrôler leur message dans l'espace médiatique. Les brochures et revues distribuées se sont avérées être trop marginales par rapport aux pouvoirs de la presse. Les messages des anarchistes étaient soit censurés ou biaisés en raison des processus éditoriaux de la presse. Les anarchistes n'ont ainsi jamais réussi à justifier et légitimer son recours à la violence à des cercles plus éloignés. Les nouvelles technologies de l'information et de la communication ont toutefois permis aux groupes terroristes de contourner plus facilement le contrôle des médias, ainsi que la censure étatique.

Pour rendre visibles leurs actions, les auteurs d'actes terroristes manient plusieurs tactiques qui s'entrecroisent (Matusitz, 2013). L'auteur explique qu'ils cherchent à faire en sorte que leurs activités opérationnelles produisent du *social noise* (par exemple la propagande par le fait) ; assimilent leurs actes à une signature (par exemple les attentats suicides, les enlèvements, les détournements d'avion, décapitations, les bombes) ; et utilisent les médias à des fins de codage (par exemple les multiples vidéos enregistrés par Ben Laden pour transmettre au monde sa mission). Ainsi, de façon plus fondamentale qu'une simple mise en mots de la contestation, le terrorisme joue sur la peur, la panique et le chaos (Matusitz, 2013). Il se peut aussi que communication et persuasion s'assemblent, lorsque les militants cherchent à soumettre les gouvernements et les institutions à leurs demandes.

Mise en spectacle de la violence

Les anarchistes de la seconde moitié du 19^{e} siècle sont la première mouvance insurrectionnelle à avoir théorisé l'usage des médias. Comme l'expliquait John Most dans le journal *Freiheit* de juillet 1885, le plus important n'est pas tant l'action en elle-même, mais l'effet de propagande qu'elle suscite. Les anarchistes ont recours à ce qu'ils appellent la propagande par le fait. Cette technique révolutionnaire est définie par Paul Brousse en 1877 dans le *Bulletin de la Fédération Jurassienne* comme « un puissant moyen de réveiller la conscience populaire » (Hubac-Occhipinti, 2015 : 155). Par la suite, les délégations de l'Association internationale des travailleurs (AIT) ont proclamé la nécessité de dépasser les formes traditionnelles de propagande écrite et verbale, relativement inefficaces. Le fait et l'action insurrectionnelle devaient compléter la propagande. Les choses se dessinaient ainsi : la nécessité de la dynamique d'un côté, et de la presse de l'autre (Wieviorka et Wolton, 1987). Bien que la propagande par le fait était considérée comme le moyen le plus efficace pour éveiller les consciences par bon nombre d'anarchistes, elle fut aussi sérieusement critiquée à

l'intérieur du mouvement (Hubac-Occhipinti, 2015 : 155). Peu à peu, au sein des différentes fédérations de libération, la propagande par le fait a été délaissée au profit d'un anarcho-syndicalisme.

Ainsi, les anarchistes auront lancé l'idée d'une propagande différente de celle qu'on avait coutume de rencontrer (Bolt, 2012). De façon corollaire, ils ont renouvelé l'utilisation stratégique des médias de groupes insurrectionnels (Wieviorka et Wolton, 1987). Faire un bon usage des médias, et de la télévision a été un objectif largement souligné par les guérillas et les mouvements révolutionnaires des années 60. Wieviorka et Wolton (1987) citent ainsi le guérillero brésilien Carlos Marighela, qui explique dans son *Mini-manuel de la guérilla* que « les mass media modernes, simplement en faisant connaître ce que font les révolutionnaires, sont d'importants instruments de propagande » (p.42).

Ce sont toutefois les premiers détournements d'avion par des militants de la cause palestinienne à partir des années 1960 qui ont marqué le début de l'histoire médiatique du terrorisme (Wieviorka et Wolton, 1987). Début septembre 1970, le Front populaire pour la Libération de la Palestine (F.P.L.P.) effectue plusieurs actes de piraterie. Certaines réussissent (le DC 8 de Swissair, le Boeing de la T.W.A. et le Jumbo-Jet de la PanAm) et d'autres échouent (le Boeing de la compagnie El Al). À l'exception du Jumbo-Jet qui a été démoli à l'aéroport du Caire, lorsque ses passagers ont été évacués, les autres ont atterri en Jordanie sur l'aéroport de Zarka. Ce dernier a été rebaptisé « aéroport de la Révolution » par les partisans du F.P.L.P. Les revendications sont claires : la libération d'otages contre la libération de fedayin emprisonnés dans plusieurs régions du monde. Dans cette affaire, le F.P.L.P. ne se limitait pas à développer une propagande par les faits. Ils excellaient aussi dans leur stratégie médiatique. Ils confectionnaient des communiqués de presse. Ils faisaient visiter à des journalistes l'aéroport. Ils ont ainsi concrétisé un modèle ; celui de la mise en scène spectaculaire d'un événement.

Le principe est donc simple. Pour ces mouvements, il faut chercher l'attention par des actions bruyantes ou controversées. Par la forme de son contenu, il doit fasciner ou effrayer le public. Aux yeux des terroristes, les choses deviennent publiques non pas seulement par la parole et la persuasion, mais aussi par la force et la violence. L'acte de violence est en quelque sorte plus riche que le symbolisme passif (Bolt, 2012). Ce qui caractérise la communication terroriste, c'est l'action elle-même. Vectrice d'attention, la violence meurtrière permet aux

auteurs d'actes terroristes de communiquer leurs messages à travers l'action qu'ils publicisent (Matusitz, 2013 ; Tuman, 2009 ; Wieviorka et Wolton, 1987). L'écho de la violence dévoile un espace d'opportunité : un choc temporaire d'un côté et une séduction de l'autre (Bolt, 2012 ; Wieviorka et Wolton, 1987). Par conséquent, l'acte violent ne se limite pas à une cible ou à un objectif unique. Il a des effets à la fois interne et externe.

À cet effet, cette stratégie néglige les principes qui fondent la communication politique (Wieviorka et Wolton, 1987). Elle percute le système de communication de l'extérieur. L'objectif du recours à la violence meurtrière est avant tout d'exercer des pressions politiques et de s'attaquer à l'ennemi. Elle cultive la menace et le chantage, en plus du désarroi et du choc émotionnel. Les auteurs d'actes terroristes enseignent, par l'amplification du spectacle de la violence, que leurs objectifs communicationnels sont incompatibles avec la communication politique des sociétés démocratiques. Car il est clair que ce spectacle ne cherche pas l'interaction, mais le choc. Ainsi, pour les auteurs, le caractère novateur du terrorisme n'est pas sa participation à la communication politique, mais bien son usage des médias.

Stratégies médiatiques

Ces mouvements travaillent constamment à développer une série de stratégies médiatiques pour accéder à la visibilité. Wieviorka et Wolton (1987) définissent les stratégies médiatiques comme « une rationalité délibérément orientée en direction de la presse » (1987 : 27). Ils peuvent diffuser des communiqués de presse ; faire circuler des fausses informations pour tromper ses adversaires ou séduire ses adhérents ; donner des entrevues clandestines ; transmettre des documents, des lettres, des confessions ou encore des enregistrements sonores ou audiovisuels de leurs déclarations pour que les journalistes les diffusent ensuite. Par ailleurs, Granjon (2009) fait valoir que les mouvements protestataires produisent également des contenus spécifiques sur le web afin de capter l'attention de journalistes. Ces ensembles de contenus sur internet sont utiles aux journalistes, dans la mesure où ils délivrent des informations supplémentaires à leur travail interprétatif. Le contenu thématique de ces inscriptions consiste habituellement à délégitimer les forces ennemies et à renforcer l'opinion favorable (Wieviorka et Wolton, 1987). Parallèlement, ils peuvent aussi faire un usage tactique des mécanismes de production de l'information. Certains groupes se calquent par exemple sur le rythme et le calendrier médiatique pour orchestrer leur action. Les auteurs

illustrent le cas des terroristes italien qui frappaient régulièrement les mercredis et les samedis. Les terroristes préféraient commettre leurs actions ces jours-là, pour la simple raison que les jeudis et les dimanches étaient les jours des plus grands tirages en Italie. En France, les poseurs de bombe de septembre 1986 ont agi en fin d'après-midi. Un choix d'heure qui n'est pas anodin, puisqu'il assurait que les journaux télévisés de 20 heures en parlent devant leur vaste auditoire.

Mais, il arrive que la presse n'obtempère pas comme des groupes d'insurgés le souhaitent. Dans le contexte des médias de masse, ces derniers peuvent être soumis à certaines règles éditoriales ou encore sous le contrôle des autorités (Wieviorka et Wolton, 1987). Par ce fait, les groupes perfectionneront leur technique de manière à imposer de force la diffusion de leur message ou à intimider les journalistes. Cela peut par exemple se traduire par l'occupation d'une station de radio ou de télévision, comme cela s'est produit dans les années 1960 et 1970 en Amérique Latine. Aussi, lors d'enlèvement, par le biais des autorités publiques, les groupes insurrectionnels peuvent demander que leurs revendications fassent l'objet d'une publication dans la presse. Dans ce processus, les insurgés peuvent appeler ou réclamer la présence des journalistes pour donner un plus large écho médiatique à leurs actions en cours. Par exemple, le Mouvement du 2 juin[14] a ordonné qu'en échange de la libération de l'important politicien allemand de l'Union chrétienne-démocrate d'Allemagne, la télévision filme en direct sa mise en liberté, ainsi que le départ en avion de six membres de l'organisation emprisonnés.

Mises en scène visuelle

Avec le développement des techniques, les groupes insurrectionnels ont de plus en plus balisé leur visibilité sur un registre iconographique et audiovisuel (El Difraoui, 2013 ; Bolt, 2012 ; Mitchell, 2011). De manière générale, le visuel joue un rôle important dans les pratiques contestataires ou étatiques (Almeida, 1995 ; Buton, 2003, 2013 ; Crettiez, 2013 ; Crettiez et Piazza, 2013a, 2013b ; Dézé, 2007, 2013). L'image a ceci de particulier qu'elle transcende les mots (Bolt, 2012). Parler visuellement fait accéder le public à un registre émotionnel fort. En raison de son efficacité, l'image s'intègre ainsi pleinement dans des systèmes de mobilisations et devient une arme de contestation redoutable (Crettiez et Piazza, 2013a).

[14] Il s'agit d'un groupe anarchiste de l'Allemagne de l'Ouest actif dans les années 1970.

L'imagerie contestataire a dans ses premiers temps été expérimentée par les socialistes du 19e siècle, pour ensuite devenir un outil de propagande de masse lors de la Première Guerre mondiale (Almeida, 1995). Images de héros, de guerre, de matériel d'artillerie, de soldats ou encore symbolisme étatique devenaient la réalité des images politiques. La propagande audiovisuelle s'est pour sa part majoritairement développée entre les deux guerres. Les partis totalitaires ont par exemple fait la promotion d'une machine de propagande visuelle sophistiquée. D'ailleurs, pour Hitler, toute propagande devait être un acte esthétique et non pas un acte rationnel.

Comme l'indique l'auteur, l'heure était aux développements d'outils visuels pour une propagande de masse. Les symboles communs devenaient la norme. La faucille et le marteau pour les communistes de l'Union soviétique ; le faisceau des licteurs de la Rome antique pour les fascistes italiens ; et la croix gammée pour les nazis. De plus, il y avait une tendance inestimable à porter une grande attention à l'image de ses chefs. Une iconographie devenue emblématique et qui a perduré dans le temps au sein de groupes d'extrême gauche et d'extrême droite (Dézé, 2007 ; Buton, 2003). Le monde visuel se normalise aussi au sein des mouvements jihadistes (El Difraoui, 2013). Ben Laden a fait des apparitions dans de nombreuses vidéos. La mise en scène était soigneusement préparée et contrôlée. Il apparaissait toujours dans les mêmes postures, avec le même ton de voix et les mêmes expressions faciales. Tout comme les nombreux travestissements de Mussolini selon son audience, Ben Laden pouvait prendre la figure de cheikh religieux, de guerrier ou d'homme d'État en fonction de ses messages et de ses événements. Parallèlement, la propagande audiovisuelle a été mise au service de sa martyrologie et d'autres images violentes, tel que les vidéos d'exécutions d'otages.

La propagande audiovisuelle peut servir plusieurs objectifs. El Difraoui (2013) explique que la stratégie audiovisuelle de Ben Laden était triple. Premièrement, afin de déclarer la guerre aux croisés et à leurs alliés Ben Laden a largement instrumentalisé les médias occidentaux et quelques médias arabes. Deuxièmement, il a mis en place une structure d'information interne pour produire et contrôler ses propres vidéos. Des vidéos, qui par un langage simple, tentent de rallier des jeunes musulmans pour qu'ils s'exilent en terre d'islam afin de vivre dans la « vraie communauté des croyants », tout en insistant sur le fait que le martyre est la seule voie du salut. Enfin, Ben Laden a misé sur l'organisation d'attentats très médiatiques. Par exemple,

les attentats contre les ambassades américaines à Dar es Salam et à Nairobi en 1998, contre le *USS Cole* en 2000, ou encore, point culminant de sa stratégie, le 11 septembre 2001.

1.3.2. Médias traditionnels : Cadrage médiatique, pouvoir et asymétrie

Les médias traditionnels ont pendant longtemps été une ressource capitale pour produire la visibilité des mouvements contestataires (Champagne, 1984, 1990, 1991 ; Gamson, 1990 ; Gamson et Wolfsfeld, 1993 ; Gitlin, 1980 ; Melucci, 1996 ; Neveu, 2015). Il a souvent été soutenu au sein de la recherche que la relation entre les médias et les mouvements était symbiotique (Clutterbuck, 1982 ; Devine & Rafalko, 1982 ; Laqueur, 1997 ; Martin, 1985 ; Nacos, 2002 ; Nelson & Scott, 1992 ; Picard, 1993 ; Powell, 2011 ; Schmid & de Graff, 1982, Van Atta, 1998 ; Wilkinson, 1997). Ces derniers supposent que les terroristes manipulent les médias pour obtenir une large publicité et que les médias dépendent d'événements dramatiques et sensationnels pour accroître leur audimat. Wilkinson (1997) précise toutefois que cela ne signifie pas que les médias cherchent à transmettre les valeurs des terroristes, mais qu'ils sont vulnérables à l'exploitation et à la manipulation des organisations terroristes. Carroll et Hackett (2006) expliquent que le risque avec ce type de perspective est de poser la question des médias et des activistes en des termes uniquement instrumentaux : les uns cherchent à faire passer le message et les autres à maximiser les profits et les parts de marché en capturant l'attention du public.

A contrario, d'autres chercheurs considèrent que la relation entre les auteurs d'actes terroristes et les médias est surestimée (Dowling, 1989 ; Paletz, Elliot et Schlesinger, 1985 ; Sleuter, 1990 ; Wieviorka et Wolton, 1987). Wieviorka et Wolton (1987) insistent par exemple sur l'indifférence qui anime certains groupes terroristes à l'égard des médias, soit parce qu'ils ne cherchent pas à effrayer la population au-delà de leurs victimes désignées, soit parce qu'ils utilisent d'autres canaux de communication. Selon d'autres études, la relation serait plus asymétrique qu'elle n'y paraît : les mouvements dépendent bien plus des médias que l'inverse. Dans cette optique, s'il est vrai que les médias requièrent des événements dramatiques et sensationnalistes pour accroître leur audimat, il n'en reste pas moins que les mouvements contestataires s'inscrivent dans un environnement concurrentiel où ils fournissent un type d'information parmi d'autres (Gamson et Wolfsfeld, 1993).

Comme de nombreuses recherches l'ont soutenu, acquérir une visibilité par le biais des médias traditionnels a souvent été préjudiciable pour les mouvements contestataires. Par

exemple, être visible via les médias traditionnels sous-tend invariablement une perte de contrôle sur le cadrage des événements (Benford et Snow, 2000 ; Gamson et Wolfsfeld, 1993). Le cadrage peut se concevoir comme « how news stories are made, i.e. how pieces of information are selected and organized to produce stories that make sense to their writers and audiences » (Ryan, 1991 : 53). Benford et Snow (2000) montrent à partir d'une série d'études que les mouvements militants n'ont que très rarement une emprise sur les histoires que les médias choisissent de couvrir et sur la manière dont ils présentent leurs revendications. Cette incapacité pour les mouvements militants à contrôler le cadrage de leur message découle en partie de deux facteurs intrinsèquement liés. Premièrement, l'information se structure à partir de contraintes commerciales et politiques dans lesquelles les journaux, la radio et la télévision fonctionnement (Bourdieu, 1996 ; Carroll et Hacket, 2006 ; Cohen, 1972). Ensuite, l'information dépend des logiques du travail journalistique en matière de routines, de ressources institutionnelles, de temps, de sélection de sources, de travail de définition du problème, etc. (Gamson, 1990).

Pour toutes ces raisons, plutôt que de produire une réalité objective du mouvement, les médias procèdent à une construction de la réalité (Hall, 1973). Comme Sleuter (1990) l'indique, aucun compte rendu des événements ne peut être une réalité écrite, car il s'agit avant tout d'une histoire particulière de la réalité. Les principales bases de ladite information objective telles que le consensus, l'équilibre, l'impartialité ou encore le professionnalisme ne peuvent se concevoir comme idéologiquement neutres. À ce titre, la recherche montre que les enjeux des mouvements sont rarement problématisés dans un cadre d'injustice (Neveu, 2015). Cela est d'autant plus vrai pour les groupes qualifiés de terroristes. Les médias traditionnels ne prennent habituellement pas en compte le contexte historique et social dans lequel les actions s'exécutent et s'attardent plutôt sur la violence.

L'action du terroriste est rarement légitimée et la plupart du temps, les terroristes sont dépeints comme des acteurs criminels violents, psychopathes ou fanatiques (Crelinsten, 1989 ; Powell, 2011 ; Sleuter, 1990). Le langage utilisé dans les médias vise ainsi à fabriquer une dichotomie entre *nous* et *eux* (Cohen, 1972 ; Sleuter, 1990). Le champ journalistique présente donc de façon unilatérale les groupes terroristes, soutenant généralement la politique gouvernementale existante (Chermak et Grunewald, 2006). Aussi, à chaque fois que surviennent des incidents terroristes, les nouvelles sont en grande partie sensationnalistes et volatiles. Dans les journaux prédominent les titres axés sur la violence, les discours des

autorités, le nombre de victimes, le rôle de la police et de l'armée et l'étiquetage négatif des groupes définis comme terroristes (Crelinsten, 1989 ; Sleuter, 1990). Les causes des terroristes sont pour leur part mentionnées brièvement, voire jamais. Paletz, Ayanian et Foazzard (1985) ont trouvé que 30 % de la couverture médiatique est axée principalement sur la violence de l'incident, 40 % est consacrée aux réponses gouvernementales et moins de 6 % se concentre sur les objectifs de ces groupes ou aux conditions sous-jacentes du conflit.

Il faut toutefois noter que la couverture des mobilisations est disparate (Neveu, 2015). À cet égard, de nombreux groupes font l'objet d'une couverture modeste, voire inexistante. Le pouvoir des médias ne s'exerce dès lors pas seulement dans le cadrage du message du mouvement, mais également dans sa capacité à exclure certains groupes du champ médiatique. Par exemple, en matière d'actes violents, les médias se sont montrés sélectifs dans les événements qu'ils ont couverts (Chermak et Grunewald, 2006 ; Crelinsten, 1989). Chermak et Grunewald (2006) ont mené une étude sur la couverture médiatique d'événements terroristes qui se sont produits sur le sol américain. Les auteurs indiquent que la plupart des Américains sont susceptibles d'être familiers avec trois ou quatre incidents terroristes survenus au cours des 25 dernières années : l'attentat du World Trade Center en 1993, à Oklahoma City en 1995, du World Trade Center et du pentagone en 2001. Pourtant, durant cette période, le FBI a recensé plus de 450 incidents qualifiés de terroristes. Les résultats des auteurs montrent que majoritairement, la plupart des incidents terroristes ne reçoivent que peu ou pas de couverture médiatique. Ce ne sont que les cas les plus sensationnalistes qui acquerront l'attention de la presse. Néanmoins, bien que Nacos (2002) soit en accord avec le fait que ce sont les actes terroristes les plus spectaculaires ou ceux qui font un nombre important de décès qui ont une couverture médiatique importante, il fait valoir que les actes mineurs peuvent également bénéficier d'une large attention selon l'emplacement, la cible et le groupe impliqué.

Cela démontre qu'avoir accès aux médias traditionnels est intimement lié aux facultés du groupe à se rendre visible (Filieule et Péchu, 1993 ; Mathieu, 2004 ; Neveu, 2010 ; Voirol, 2005b) et à développer des « stratégies d'intéressement » (Granjon, 2009) :

> They must struggle to establish it, often at what they regard as serious costs for the message that they wish to convey. Their dependency forces them to pay a price of entry that affects the subsequent transaction in various ways. (Gamson et Wolfsfeld, 1993 : 117)

Les auteurs expliquent que dans ce contexte, l'un des principaux enjeux pour les activistes est de condenser le message de la façon la plus efficace possible pour éviter qu'il soit dénaturé par les médias de masse. Le fait de devoir obtenir une couverture médiatique tout en gardant le message initial pousse les mouvements à adopter des stratégies spécifiques. Partant du constat que le spectacle fait généralement les gros titres des journaux, les mouvements mettront l'accent sur des stratégies d'action qui valorisent le sensationnalisme, le drame et la confrontation, comme nous l'avons soulevé dans la section précédente.

1.3.3. Internet : Entre indépendance, manipulation de l'attention et viralité

L'arrivée d'internet et du web 2.0 a marqué une nouvelle mutation dans l'économie de l'attention des mouvements (Tufekci, 2013). L'une des transformations majeures découle du fait que les activistes peuvent maintenant produire et distribuer leur cause de façon indépendante (Micó et Casero-Ripollés, 2014). Les groupes contestataires sont maintenant en mesure de délivrer une grande quantité d'information à travers les sites de réseaux sociaux, en permettant le téléchargement de leur brochure et autres contenus (Neveu, 2009). Comme nous l'avons largement souligné, le web 2.0 se caractérise par un haut degré d'interactivité et de contenu généré par l'utilisateur. Internet offre ainsi aux mouvements sociaux la possibilité de diffuser leur message sans faire l'objet d'une vérification tatillonne (della Porta et Mosca, 2005). Le contenu fera l'objet d'une suppression seulement dans le cas où il serait signalé à l'entreprise propriétaire qui décide en dernier ressort de retirer ou de maintenir le contenu en ligne (Cardon, 2015).

Par ce fait, Della Porta et Mosca (2005) notent qu'internet se distingue des médias traditionnels, car il favorise la *disintermediation* où les « movements present themselves directly to the general public with low costs especially facilitating resource-poor actors » (p.166). En s'émancipant des médias traditionnels ou d'organisations officielles, les militants sont susceptibles de se connecter les uns aux autres selon leurs propres termes et de propager plus largement leur message (Tufekci, 2013). L'auteure ajoute toutefois que rendre davantage visible un message à un large public renforce la possibilité de *clash* entre audiences, particulièrement lorsque le groupe en question utilise un langage offensant.

Si l'apport quantitatif et qualitatif est indéniable, il vaut la peine d'indiquer que les formats médiatiques se trouvent quant à eux transformés. Bien que la diffusion se fait plus facilement, cela n'empêche que les groupes doivent s'efforcer de mettre en place des pratiques autopromotionnelles à la fois complexes et virtuoses (Cardon et Granjon, 2010). Pour les auteurs, la visibilité en ligne des activistes n'échappe pas à des guerres de visibilité. Se faire entendre sur la toile nécessite de mettre en place des stratégies pour obtenir la reconnaissance des autres internautes afin qu'ils puissent avoir la plus grande visibilité possible. Tout comme avec les médias traditionnels, les militants doivent construire une audience afin de donner écho à leur message. Il existe ainsi de multiples manières d'agir dans l'espace d'apparence afin que les messages atteignent une forte visibilité : le détournement subjectif et parodique ; la viralité ; et l'automatisation.

Cardon et Granjon (2010) indiquent qu'au sein de cette nouvelle culture participative, les échanges s'énoncent davantage à la première personne, font place aux affects et aux ressentis et introduisent une part plus forte de détournements ironiques. Cette réarticulation du subjectif dans les cadres médiatiques marque ainsi une atténuation des frontières entre l'information, le divertissement et la personnification des événements. Dans ce contexte, les auteurs font valoir que la source immédiate des pratiques informationnelles des militants devient celle de la dérision, du détournement symbolique et de la cacophonie. Ces méthodes ont pour particularité d'augmenter les chances que leurs messages deviennent viraux.

Internet offre plusieurs possibilités aux mouvements de créer une attention forte autour de leur mobilisation dans le but qu'il soit impossible de les ignorer (Tufekci, 2013). Les activistes apprennent à galvaniser l'attention en utilisant plusieurs procédés qui se rangent du côté de tous les phénomènes viraux sur internet (Mina, 2019). À ce titre, Fung et Shkabatur (2015) qualifient de *viral engagement* les messages politiques ou les campagnes « that spreads quickly, reaches large audiences, and calls for action » (p.155).

Dernièrement, cette capacité à manipuler l'économie de l'attention a particulièrement été documentée au sein de militants d'extrême droite et d'autres sous-cultures internet (par exemple, conspirationnistes, mouvements pour les droits des hommes, gamergaters, alt-right) (voir par exemple Benkler et al., 2018 ; boyd, 2017 ; Marwick et Lewis, 2017 ; Phillips, 2015, 2018). Ces stratégies de manipulation ont toutefois fait l'objet d'une attention moindre dans la

littérature en ce qui concerne d'autres formes d'extrémismes, comme le jihadisme, préférant axer la recherche sur la manière dont ces groupes utilisent internet à des fins terroristes.

Ces mécanismes de viralité et de contagion technico-sociales sont régulièrement incarnés par les mèmes numériques (Nissenbaum et Shifman, 2017 ; Philips et Milner, 2017 ; Shifman, 2013a, 2013b). L'idée de mème a été originairement proposée par le biologiste Richard Dawkins (1976) qui établit une équivalence structurelle entre le code génétique et la circulation de l'information qui se propage de personnes à personnes. S'inspirant de la biologie évolutionniste, l'auteur décrit la manière dont les « units of cultural transmission » (1976 : 206) sont dotées de capacités de réplication et de mutation.

À la suite de Dawkins, la métaphore du mème a trouvé une forte résonnance auprès des participants sur internet et s'est rapidement imposée pour décrire les plaisanteries, les slogans, les habitudes idiosyncrasiques et la tendance des participants à légender d'innombrables photos de chat (Philips et Milner, 2017 ; Shifman, 2013a). Or, si le phénomène des mèmes est souvent associé à des images humoristiques, ils sont bien plus complexes qu'ils n'y paraissent. Milner (2016) exprime l'idée que les mèmes sont des expressions vernaculaires qui font écho à plusieurs genres de communications et degré de médiation. Les mèmes peuvent prendre des formes infinies et exister sur plusieurs types de médias (Mina, 2019). Malgré ces divergences, Philips et Milner (2017) soulignent que les mèmes sont unis par une même logique :

> They depend on *multi-modality* (expression through diverse modes of communication, including written words and static images, as well as audio and video), *reappropriation* (the remix and recombination of existing cultural materials), *resonance* (the manifestation of strong personal affinity), collectivism (social creation and transformation), and *spread* (circulation through mass networks) (p.31).

Étant donné que les mèmes sont simples à déployer, entraînent une culture partagée et conduisent à plus de visionnement, il n'est pas étonnant que ces derniers aient été de plus en plus utilisés à des fins de militantisme politique (Bennet et Segerberg, 2012 ; Bogerts et Fielitz, 2019 ; Huntington, 2016 ; Kligler-Vilenchik et al., 2016 ; Mina, 2014, 2019 ; Miller-Idriss, 2019 ; Milner, 2013, 2016 ; Shifman, 2013a). Ces micro-actions sont avantageuses pour les groupes militants, car ils permettent de générer répétitivement des messages et des affirmations (Mina, 2019 : 21). Pour l'auteur, les mèmes numériques ont ainsi un fort

potentiel pour soutenir un processus appelé la « *synchronization of opinion*[15] » (Mina, 2019 : 21).

Si les mèmes développent un narratif ou un cadrage apte à incarner des phénomènes viraux, qu'en est-il plus exactement de la diffusion ? En d'autres termes, comment les mèmes peuvent-ils atteindre une propagation virale ? Fung et Shkabatur (2015) expliquent que la viralité découle du fait que les technologies numériques se distinguent par leur capacité à faciliter la circulation de l'information et de la diffuser rapidement auprès d'un vaste bassin d'utilisateurs. Les réseaux sociaux par exemple sont conçus pour réduire considérablement le coût de certaines actions par des fonctionnalités comme le *like* ou encore le *partage* de contenus. Cette dernière génération de fonctionnalités informatiques accroît dès lors les chances qu'une campagne politique puisse devenir virale. Les auteurs font remarquer que de telles pratiques s'étendent facilement à des citoyens-amateurs qui peuvent s'engager dans la participation politique.

Par ailleurs, ces phénomènes viraux peuvent aussi être amplifiés par le déploiement massif de *social botnets,* comme cela a pu être observé dans plusieurs contextes politiques (voir par exemple Abokhodair et al., 2016 ; Benkler et al., 2018 ; Bessi et Ferrara, 2016 ; Berger et Morgan, 2015 ; Brachten et al., 2017 ; Forelle et al., 2015 ; Hegelich et Janetzko, 2016 ; Howard et al., 2016 ; Howard et Kollanyi, 2016 ; Marwick et Lewis, 2017 ; Schäfer et Heinrich, 2017 ; Stukal et al., 2017). Par exemple, lors des élections présentielles américaines de 2016, les *social botnet*s auraient été responsables d'environ un cinquième de la conversation sur Twitter (Howard et al., 2016). Les *social botnets* peuvent se définir comme des scripts automatisés, qui tentent d'imiter le comportement humain et interagissent sur des plateformes de médias sociaux (Hwang et al., 2012 ; Wolley, 2016). Ces derniers temps, les social *botnets* sont devenus réputés pour diffuser de la « propagande computationnelle »[16] (Woolley et Howard, 2017 ; Woolley, 2016) et relayer des « messages astroturfs[17] » qui

[15] L'auteure emprunte cette expression à Tom Standage, dans son ouvrage « Writing on the Wall : Social Media-The First 2,000 Years » (2013).

[16] La propagande computationnelle est un terme qui : « encompasses recent digital misinformation and manipulation efforts. It is best defined as the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks (Woolley et Howard, 2016). Computational propaganda involves learning from and mimicking real people so as to manipulate public opinion across a diverse range of platforms and device networks » (Woolley et Howard, 2017 :6).

[17] L'astroturfing en ligne « refers to coordinated campaigns where messages supporting a specific agenda are distributed via the Internet. These messages employ deception to create the appearance of being generated by an independent entity. (…) The key component of astroturfing is the creation of false impression that a particular idea or opinion has widespread support » (Zhang, Carpenter et Ko, 2013 : 1).

donnent l'illusion d'un faux sentiment de soutien ou de consensus sur une idée particulière (Murthy et al., 2016 ; Ratkiewicz et al., 2011 ; Woolley et Howard, 2016a, 2016b).

Si les *botnet*s se sont multipliés au sein de différents contextes politiques lors des dernières années, c'est entre autres parce qu'il s'agit de programmes informatiques polyvalents, peu coûteux à produire et en constante évolution (Abokhodair et al., 2015 ; Woolley et Howard, 2016b). Les *social botnets* sont particulièrement répandus sur Twitter du fait de leurs caractéristiques techniques et de l'ouverture de ses interfaces de programmation (API) (Chu et al., 2010 ; 2012). Néanmoins, ce phénomène n'est pas restreint à Twitter et a pu être observé sur de nombreuses plateformes numériques comme Facebook, Reddit, Telegram ou encore Wikipedia (Lokot et Diakopoulos, 2016). Bien que le degré de satisfaction varie indéniablement d'un *bot* à l'autre et dépend du rôle qui lui est octroyé, la recherche s'accorde à dire qu'ils deviennent de plus en plus sophistiqués, rendant par conséquent leur détection plus ardue (Ferrara et al., 2016).

1.3.4. Un média ou des médias ? Rétablir l'écosystème médiatique des activistes

Les études qui se sont intéressées au lien entre technologies numériques et activisme ont eu tendance à porter leur attention sur un seul type de média (sites web, blogs, plateformes de réseaux sociaux) (voir par exemple Cammaerts, 2008 ; Della Porta et Mosca, 2005 ; Harlow, 2012 ; Stein, 2009, van Aelst et Walgrave, 2004). Ces travaux disqualifient d'une certaine manière les nombreuses ramifications entre plusieurs technologies, acteurs et pratiques qui permettent à l'action collective de se produire (McCurdy, 2011 ; Mattoni, 2009 ; Meikle, 2002 ; Padovani, 2010 ; Treré, 2012, 2018 ; Treré et Mattoni, 2016). Treré (2012) soutient qu'il est nécessaire de dépasser le parti pris d'un média unique pour étudier la protestation en ligne, car « it can reduce the complexity of the internet to just one of its comprising technologies, or to certain particular « portions » of this complex environment » (p. 2362). Pour l'auteur, ne s'intéresser qu'à une partie du scénario technologique évincerait une multitude d'autres aspects nécessaires à la compréhension de l'activité en ligne d'un mouvement social et par conséquent la dynamique de l'action collective.

Il fait ainsi la proposition d'une approche plus holistique en adoptant la perspective de la théorie de l'écologie des médias. L'objectif de cette perspective est de tenir compte de l'ensemble des technologies de communication avec lesquelles les activistes interagissent lors de manifestations et de mobilisations. Plusieurs études ont d'ailleurs montré comment les

mouvements se servaient de plusieurs technologies à la fois (voir par exemple Dahlberg-Grunberg, 2016 ; Goddard, 2011 ; Kahn et Kellner, 2008 ; Poell, 2014 ; Srinivasan et Fish 2011 ; Tufekci et Wilson, 2012 ; Treré, 2012). Ces recherches restaurent la complexité communicative des mouvements sociaux en explorant « the multiplicity, the interconnections, the dynamic evolution of old and new media forms for social change » (Treré et Mattoni, 2016 : 291). Cela démontre d'une certaine manière que la littérature récente témoigne de la nécessité d'aborder l'action collective en ligne par rapport aux médias dans son ensemble (Treré, 2012). Le fait de reconnaître et d'explorer la multiplicité des formes et pratiques médiatiques permet de dépasser la dichotomie coutumière entre nouveaux et anciens médias (Chadwick, 2017 ; Dahlberg-Grunberg, 2016 ; McCurdy, 2011 ; Srinivasan et Fish, 2011 ; Tufekci et Wilson, 2012 ; Treré, 2018 ; Treré et Mattoni, 2016).

Pour conclure, McCurdy (2011) indique qu'au sein de l'environnement numérique les mouvements sociaux n'utilisent pas les anciens médias d'un côté ou les nouveaux médias de l'autre. Au contraire, l'auteur atteste qu'il existe une convergence entre une multitude de médias de masse et de technologies numériques, formant par conséquent un environnement médiatique large. De même, Tufekci et Wilson (2012) dans leur étude sur la révolution égyptienne de 2011, rappellent que les médias sociaux ne représentent qu'une portion du système de communication politique en Afrique Nord et Moyen-Orient. De fait, « the connectivity infrastructure should be analyzed as a complex ecology rather than in terms of any specific platform or device » (Tufekci et Wilson, 2012 : 365). Ce système de communication politique comprend une série de composantes interdépendantes qui mélangent à la fois les médias traditionnels, les technologies numériques et l'accroissement de la téléphonie mobile qui a sans conteste amélioré la communication par de nouvelles capacités de diffusion d'images et de vidéo. Pleyers (2013) note quant à lui à partir d'une série d'études que dans plusieurs manifestations de grandes ampleurs (par exemple le Printemps arabe et le mouvement *Occupy*), les médias de masse ont constitué des relais essentiels aux causes exprimées sur les médias sociaux.

Ainsi, dans une telle dynamique les pratiques des activistes mêlent perpétuellement un vaste ensemble de médias, allant de technologies numériques plus anciennes (forums et courriels) à des médias plus traditionnels (radios, télévision, presse) (Treré, 2018). Cela démontre que si internet permet de nouvelles pratiques de visibilité et d'attention, elles ne se substituent toutefois pas aux médias traditionnels. Elles s'articulent au contraire avec eux (Cardoso,

2012 ; Tufekci, 2013 ; Pleyers, 2013). Ces études affirment que les médias traditionnels restent un vecteur important de visibilité publique. En utilisant internet, les groupes peuvent plus facilement définir leurs messages et attirer l'attention sur eux (Tufekci, 2013). Dès lors, internet est efficient pour faire remonter l'information jusqu'aux médias de masse, qui leur donne en retour la possibilité d'acquérir une plus grande visibilité. Cette relation n'est toutefois pas asymétrique, explique Pleyers (2013). A contrario, les médias traditionnels représentent une source non négligeable pour alimenter les messages sur les réseaux sociaux et les sites militants. Cela démontre à quel point le paysage médiatique des activistes se bâtit à partir de la superposition et l'articulation de différents médias et technologies.

1.4. Activisme et participation en ligne

Jusqu'à présent, nous avons abordé la relation des médias et des mouvements militants. Dans cette section, nous aborderons les dynamiques de mobilisation en ligne. Comment se mobilise-t-on en ligne ? Quelles sont les formes d'engagement ? Qu'est-ce qu'internet fait aux mobilisations ? Pour tenter de répondre à ces questions, cette section portera sur trois axes. Le premier s'intéressera à la manière de faire groupe en ligne et de diffuser l'information. Le second concernera les travaux qui se sont intéressés aux effets d'internet sur les mobilisations. Nous verrons que ces travaux ont la plupart du temps envisagé cette question en assumant la dématérialisation comme caractéristique première des technologies numériques, renforçant par conséquent la distinction entre sphère physique et sphère digitale. Cette lacune sera toutefois soulevée et en partie dépassée par un ensemble de travaux qui ont restitué les mobilisations dans une interaction complexe entre le numérique et le non numérique. Cela fera l'objet de notre troisième section.

1.4.1. Les mobilisations de clavier

Nous avons vu que toute action collective découle d'un partage d'intérêts communs et de la construction d'une identité collective. À partir de là, les militants se rassemblent autour d'un monde commun. Ce monde commun rassemble, en même temps qu'il crée un « sens public » (Cefaï et Pasquier, 2003). Les participants s'engagent alors en vue de modifier une situation. L'une des particularités d'internet est que l'action collective peut se dérouler sans avoir forcément développé un sens d'appartenance a priori (Cardon, 2010). Si internet offre à tous

un lieu d'apparence, les luttes deviennent, pour leur part, davantage individualisées (Cardon et Granjon, 2010 ; Badouard, 2013).

Par ce fait, les individus investis dans une cause ne sont plus nécessairement reliés de manière tangible à un collectif (Badouard, 2013). Cela a pour effet d'engendrer des formes d'engagement de plus en plus disparates et d'intensifier une individualité aux dépens d'un partage de référentiels communs. Ils opèrent entre autres par des forces de coopérations faibles, qui dans certains cas, se solidifieront à force de consolider et renforcer les liens et les valeurs d'un groupe (Cardon, 2010). Ces « mobilisations de clavier » laissent par conséquent place à des actions parfois peu coordonnées (Badouard, 2013).

L'auteur ajoute qu'en raison de son individualisation, les mobilisations de clavier ne sont nullement le fait d'activistes ordinaires, mais concernent aussi tous les autres citoyens. En d'autres mots, il n'existe pas un type de formalisation en ligne. Comme l'indique Cardon (2010) ces formes d'action peuvent donner l'illusion d'être fragile et inorganisée. Or l'auteur souligne qu'il serait vain d'opposer le militantisme en ligne à des « vraies » actions collectives durables et organisées. À cet égard, l'auteur indique que les formes de coordinations sur internet combinées à des actions collectives du monde réel (souvent elles-mêmes hétérogènes et multiples) ont montré des formes d'engagements concrets et efficaces. C'est par exemple avec le Réseau Éducation Sans Frontières (RESF) ou la mobilisation contre la loi Hadopi.

Ces nouvelles formes d'engagement effectuent le passage d'un militantisme traditionnel à un « engagement distancié » (Granjon, 2003). Se renouvellent ainsi des modes d'action collective et de formes de sociabilité. Ils opèrent selon un modèle de structure en réseau. Leurs formes d'expression se diffusent parmi de multiples voix, dont chacune est porteuse d'une singularité. S'engager s'effectue dans une multitude de projets qui sont conduits de manière collective ou individuelle. Les militants peuvent exploiter le potentiel de communication lié aux plateformes numériques, construire des interfaces numériques (sites web, lettres d'information, listes de diffusion, etc.) ou encore déployer des pratiques soutenues au sein des réseaux. Les actions en ligne ont ceci de spécifique : elles peuvent partir d'une série de points multiples et indéterminés sur le web (Cardon, 2010). Un moyen efficace qui permet aux mobilisations en ligne de rendre visible leur argumentaire.

Mais, au-delà, les militants en ligne devront développer des compétences pour faire circuler le flux informationnel, créer des liens et s'engager avec d'autres militants et dans d'autres projets (Granjon, 2003). Pour l'auteur, l'une des qualités essentielles dont doit se munir tout activiste en ligne est l'adaptabilité. Cette adaptabilité amende les possibilités de tirer profit d'événements qui permettraient la réussite de la contestation. Une des conditions nécessaires de cette flexibilité s'articule dans la capacité à transmettre et faire circuler l'information. Granjon (2003) relève trois types d'acteurs fortement investis dans ces opérations de propagation de l'information : les passeurs, les filtreurs et les interprètes.

Les passeurs sont sans conteste la catégorie de militant-internaute la plus nombreuse. Leur fonction est de faire circuler sur les plateformes numériques l'ensemble des informations formelles ou informelles qui se construisent dans les cercles militants restreints. Ils rendent lisible la protestation, en propageant et reconstituant des informations fragmentées qui feront l'objet d'une lecture. Au-delà, ils édifient une partie de la mémoire du mouvement social en conservant les traces discursives. Les passeurs seraient ainsi « un outil mnémotechnique de réflexivité, de décision et d'auto-organisation » (p.4).

Les filtreurs ont pour leur part un rôle de catalyseur, face à la pléthore d'informations disponibles. Ces militants-internautes, qui s'investissent aussi dans la distribution d'information, auraient un rôle supplémentaire. Ils ciblent et sélectionnent afin de soulager cognitivement les autres militants-internautes. Les interprètes peuvent être considérés comme des « aides cognitives » en aidant à la gestion et à l'appropriation des contenus diffusés. En d'autres termes, ils orchestrent un registre d'idées en couplant plusieurs écrits et sources et en les analysant.

Il reste toutefois un point aveugle à éclaircir, comment ces internautes-militants s'engagent-ils dans des formes d'action collective en ligne ? À ce titre, Akrich et Méadal (2007) notent à partir de leur étude sur l'engagement de personnes dans des listes de discussion, trois niveaux d'action collective. Le premier renvoie aux actions individuelles qui recherchent la reconnaissance collective. Il s'agit de militants qui ne s'inscrivent pas dans la construction d'un projet partagé, mais tentent à titre individuel de faire connaître leurs actions à un mouvement. Ils fondent en quelque sorte une identité collective commune, sans adhésion formelle. Chaque participant peut être représentant de la cause et parler en son nom propre pour les autres. Ensuite, il y a l'agrégation d'actions individuelles. L'enjeu est cette fois-ci

d'établir une opinion commune ou une action collective, à partir d'individus qui agissent isolément. La somme des actions aura donc pour but de produire un effet de masse. Enfin, il y a la structure collective, qui établit des actions collectives à partir de groupes formés en amont.

1.4.2. Le rôle d'internet dans les mobilisations

Si l'usage d'internet dans les mobilisations politiques a attisé l'intérêt des chercheurs dès les années 1990 (Garrett, 2006), ce champ de recherche s'est considérablement développé dans les années 2000 (Chadwick et Howard, 2010 ; Pleyers, 2013). Cette question a été balisée au sein de diverses disciplines, se trouvant au confluent de disciplines variées, telles que la sociologie, la science politique ou encore les études en communication. Face à cette diversité d'ancrage théorique et méthodologique, les études scientifiques qui interrogent les effets de la médiation numérique sur les logiques de mobilisation, demeurent fragmentées et ont suscité un certain nombre de controverses au cours des dernières années (Foust et al., 2017 ; Garrett, 2006).

Le point de désaccord s'articule essentiellement autour de l'ampleur du rôle d'internet dans les mobilisations, oscillant entre un optimisme utopique (Shirky, 2008, 2011) et un scepticisme obstiné (Morozov, 2012). Pour la première conception, qui s'est particulièrement renforcée lors du printemps arabe, internet a parfois été présenté caricaturalement comme une « révolution 2.0 » (Ghonim, 2012). Cette conception, prédominante dans la sphère journalistique notamment, fut mise à rude épreuve par le fait qu'internet pouvait exercer un pouvoir de surveillance et de contrôle sans précédent (Morozov, 2012). Comme le stipule Farrell (2012), ces approches sont problématiques, car elles sont peu étayées par des théories qui lient internet et démocratie. Dès lors, « those who believe that the internet helps democracy can point to one set of relationships, whereas those who believe that it hurts can point to another » (Farrell, 2012: 38). Cette dichotomie entre utopie et critique s'est exercée dans de nombreux travaux en ciblant le débat sur les potentiels effets de nouveautés introduits par l'usage du numérique au sein de l'activisme politique. Trois thèmes se démarquent ainsi de la littérature : l'hypothèse du renforcement, l'hypothèse de l'innovation et les théories critiques.

Internet comme facilitateur de l'action collective

Cette thèse partage l'idée qu'internet est un facilitateur de l'action traditionnelle, sur les plans de la mobilisation, de l'organisation et de la transnationalisation (van Laer et van Aelst, 2010). Les tenants de cette thèse affirment que la technologie favorise une réduction du coût de la participation (Bimber, 2003 ; Della Porta et Mosca, 2005 ; Earl et Kimport, 2011 ; Mosca et Della Porta, 2009 ; Postmes et Brunsting, 2002 ; Rheingold, 2003 ; Shirky, 2008). Cette facilitation repose sur les nombreux avantages qu'offre internet aux militants tels que l'accessibilité et le coût ; l'anonymat ; l'absence de censure a priori ; la vitesse et l'immédiateté ; l'interactivité (Awan, 2007b ; Bockstette, 2009).

Selon de nombreux travaux, l'avènement de ces formes alternatives de communication viendrait ainsi faciliter le recrutement, la formation d'une identité collective, la coordination et donc la participation politique du groupe (Arquilla et Ronfeldt, 2002 ; Bennett et al., 2008 ; Diani, 2000 ; Gurak, 1997 ; Mercea, 2012 ; Leizerov, 2000 ; van Aelst et Walgrave, 2002). Par ailleurs, d'autres études (Ayres, 1999 ; Elin, 2003 ; Myers, 1994) ajoutent que cette capacité à connecter et à coordonner plus facilement des personnes dispersées géographiquement permet l'émergence de réseaux transnationaux.

L'assertion qui résume sans doute le mieux cette position a été formulée par van Aelst et Walgave (2002) qui soutiennent que « participation in politics will have been facilitated through the use of ICTs. Political action is made easier, faster and more universal by the developing technologies. ICTs lower the costs and obstacles of organizing collective action significantly » (p.446). Toutefois, certaines études sont venues nuancer ce propos. Earl et Kimport (2011) ont raison de faire remarquer que la capacité des nouvelles technologies à faciliter la mobilisation ne s'exerce que dans certains contextes politiques et pour certaines formes de participation. La plupart des revendications en ligne dépendront en grande partie de la manière dont les militants utilisent la technologie et se l'approprient (Loader et Mercea, 2011).

Internet comme créateur de nouvelles formes d'activisme

La seconde thèse établit qu'internet génère de nouvelles formes d'action collective. Au sein de la littérature, cette thèse donne lieu à deux principales hypothèses. La première postule qu'internet promeut de nouvelles formes de résistance (Bennett et Segerberg, 2012 ; Cardoso

et Pereira Neto, 2004 ; Mercea, 2012 ; Rolfe, 2005 ; van Laer et van Aelst, 2009 ; Shirky, 2008, 2011 ; Theocharis, 2013). Par exemple, dans son analyse sur les mobilisations qui ont suivi la mort de l'avocat Rodrigo Rosenberg au Guatemala, Harlow (2012) montre comment par le biais de Facebook des dizaines de milliers de guatémaltèques se sont rassemblés hors-ligne afin de réclamer justice. L'auteur indique que son étude met en avant une dimension trop souvent négligée dans la littérature sur l'activisme en ligne, à savoir qu'internet a la capacité de créer et pas seulement de renforcer l'activisme politique.

Dans cette même lignée, Bennett et Segerberg (2012), à partir de trois phénomènes protestataires (le printemps arabe, les Indignados espagnols et la mouvance Occupy), indiquent que l'action collective s'accompagne maintenant d'une logique « d'action connective ». Les auteurs stipulent que « at the core of this logic is the recognition of digital media as organizing agents » (p.752). Dans leur étude, les auteurs montrent comment les technologies numériques sont vectrices de nouvelles possibilités, en permettant aux militants de mieux s'organiser et de mieux identifier les problèmes sociaux. Dans la logique de l'action connective , la participation à l'action protestataire est le fruit d'une appropriation individuelle des médias sociaux et d'une diffusion en ligne de cadrages et d'interprétations personnelles. L'action connective est ainsi le lieu d'une libre association où s'organise le partage d'idées et d'actions dans le cadre de relation de confiance. Selon cette perspective, l'action se fonde « sur le consensus ad hoc plutôt que sur des engagements idéologiques préexistants » (Loveluck, 2016 : 331).

La deuxième hypothèse identifiée met en avant les nouveaux outils exclusivement basés sur internet qui permettent aux militants d'appuyer leur revendication (Earl et Kimport, 2010 ; Juris, 2005 ; van Laer et van Aelst 2010 ; van de Donk et al., 2004). Plusieurs études estiment que si internet facilite des formes plus traditionnelles d'action collective, il encourage aussi de nouvelles formes de protestation en ligne (Costanza-Chock, 2003 ; van Laer et van Aelst, 2010). Ce faisant, internet aurait considérablement étendu le répertoire d'action collective (Tilly, 1984) des mouvements contemporains (McAdam et al., 2001). Certains auteurs parlent d'un « repertoire of electronic contention » (Costanza-Chock, 2003 ; Rolfe, 2005). Ces activités peuvent aller de la pétition en ligne à des *sit-in* virtuels, en passant par le *hacking*, des campagnes par courrier électronique, des boycotts, ou encore des campagnes de financement (Mercea, 2012 ; van Laer et Van Aelst, 2010). Ainsi, pour la plupart des répertoires « of electronic contention », qui prennent la forme d'*e-tactics* (Earl et Kimport,

2011), il s'agira d'« amplify and extend "traditional" movement communications efforts » (Costanza-Chock, 2003 : 3). Plus que de remplacer les tactiques de mouvement social existantes, internet viendrait ainsi les compléter (van de Donk et al., 2004).

Internet et théories critiques

Au-delà des thèses plus optimistes, au sein de la recherche existe une réserve critique quant au rôle que jouerait internet dans les mobilisations (Bimber, 2001, Diani, 2000 ; Scheufele et Nisbet, 2002 ; van de Donk et al., 2004). Selon les points de vue abordés, certains s'interrogent sur l'influence réelle d'internet dans la transnationalisation des mouvements, d'autres se demandent si les internautes qui soutiennent une mobilisation sont réellement dédiés à la cause (Harlow, 2012). Mais dans tous les cas, l'objectif est de déconstruire la rhétorique enthousiaste concernant les nouvelles formes d'activisme subséquentes aux technologies numériques. Parmi les perspectives les plus pessimistes, on retrouve le concept de *slacktivism* (Morozov, 2009a, 2009b ; Gladwell, 2010), peu étayé empiriquement, mais qui a toutefois suscité de vifs débats (Christensen, 2011). D'emblée, le *slaktivism* représente une forme d'activisme dénué de sens et sans signification. Ce terme fait référence à l'idée que les pratiques en ligne n'auraient aucune incidence sur les décisions et résultats politiques (Morozov, 2009a, 2009b). Pour l'auteur, elles permettraient uniquement d'accroître le sentiment de bien-être des participants en les laissant penser qu'ils contribuent au jeu politique.

De nombreux travaux ont toutefois été moins pessimistes que n'ont pu l'être les tenants du *slacktivism*. Tout en reconnaissant qu'internet favorise de nouvelles possibilités d'action collective, ces recherches exprimeront leur scepticisme quant à la durabilité et à la stabilité des actions en ligne (van Aelst et Walgrave, 2002). Ce point de vue défend l'idée qu'internet renforce la mobilisation de mouvements déjà existants, plutôt que d'entraîner de nouvelles formes de mobilisation. L'une des principales préoccupations de ces études s'articule autour de la question de savoir si sur base de contacts en ligne un mouvement serait en mesure d'être généré.

À ce titre, pour plusieurs chercheurs (McAdam et al., 1996 ; Diani 2000), l'avènement d'internet ne présage en rien l'apparition de mouvements sociaux transnationaux. Leur principale critique repose sur le fait que créer de nouveaux liens sur une base uniquement virtuelle est limité. Diani (2000) reconnaît sans conteste que l'utilisation d'internet favorise

une communication organisationnelle, toutefois il estime que les réseaux de mobilisation dépendent essentiellement d'interactions quotidiennes face à face, primordiales à la diffusion de l'action collective. En somme, pour l'auteur, les liens et les solidarités existants dans le monde physique sont plus déterminants dans les tentatives de mobilisation que les technologies numériques. Entre autres, l'interaction face à face procure des niveaux de confiance entre les participants bien plus solides que les technologies numériques. C'est justement cette solidification des niveaux de confiance qui sera en mesure de maintenir une action collective durable. Les études ont alors commencé à soutenir qu'une combinaison d'interaction face à face et en ligne était préférable pour créer et maintenir un mouvement (Etzioni et Etzioni, 1999 ; Pickerill, 2003 ; van Laer, 2010).

Un autre axiome de la critique de Bimber (2001, 2003) est que l'augmentation d'informations n'implique pas nécessairement que les internautes puissent la traiter efficacement. Autrement dit, internet ne prédit en rien que les internautes auraient une meilleure compréhension de la politique qui les pousserait à une plus grande participation (par exemple au vote, au débat politique ou encore à la participation à des rassemblements). Pour toutes les raisons évoquées ci-dessus, Marichal (2013) estime que l'activité politique en ligne doit se comprendre comme un activisme à petite échelle ou plus particulièrement comme un type de *micro-activisme*.

1.4.3. Sortir du dualisme numérique

Le problème avec la plupart des études exposées ci-dessus est qu'elles maintiennent une nette distinction entre la sphère physique et la sphère numérique. Un certain nombre de chercheurs (Castells, 2007 ; Gerbaudo, 2012 ; Kinsley, 2014 ; Poell, 2014 ; Sassen, 2002 ; Jurgenson 2012) se démarqueront de ces différents discours en dépassant ce que Jurgenson (2012) appelle le « dualisme numérique ». Jurgenson propose que les nouvelles technologies « effectively *merge* the digital and physical into an *augmented reality* » (2012 :84). Appliqué au militantisme, l'auteur parle d'une « *augmented revolution »* :

> It is this massive implosion of atoms and bits that has created an augmented reality where the advantages of digitality- information spreads faster, more voices become empowered, enhanced organization and consensus capabilities- intersect with the importance of occupying physical space with flesh-and-blood bodies » (p.86).

Pour plusieurs auteurs, les technologies numériques supplémentent le réel, plus qu'elles ne le remplacent (Woolgar, 2002 ; Jurgenson, 2012). Allant dans un sens similaire, Sassen rappelle que « producing capital mobility takes capital fixity » (2002 : 369). En considérant que l'hyper-mobilité et la dématérialisation sont les caractéristiques premières des technologies numériques, l'auteure fait remarquer que la plupart des études ont exclu les variables « non-digitales » de leur analyse. Or, comme le soulignent certains auteurs (Sassen, 2002 ; Poell, 2014), il est nécessaire d'appréhender les technologies numériques comme des assemblages complexes, où s'entremêle un ensemble de configurations technico-culturelles et de systèmes de pouvoir politique et économique en ligne et hors-ligne.

Inévitablement, le fait d'envisager le numérique et le non numérique comme étant intriqués a amené les travaux à remettre en question la dichotomie entre le local et le global. Plusieurs protestations (par exemple le mouvement Occupy Wall Street qui s'est par la suite internationalisé) montrent que malgré un usage abondant du web dès leur début, occuper l'espace physique est resté une dimension essentielle (Jurgenson, 2012). Ainsi, « through the Internet, local initiatives become part of a global network of activism without losing the focus on specific local struggles » (Sassen, 2002 : 380). Malgré la « globalisation » des mouvements, ceux-ci continuent de s'ancrer dans leurs contextes locaux et dans leurs interactions physiques (Castells, 2007).

Cela fait nettement écho aux travaux de Gerbaudo (2012) qui dans son ouvrage *Tweets and the Streets* montre à partir de trois études de cas (la révolution égyptienne de 2011, le mouvement des indignés en Espagne et Occupy Wall Street) comment les médias sociaux articulent une *choreography of assembly*. Les médias sociaux permettent ainsi de construire un espace symbolique qui facilite et guide les manifestations dans l'espace physique d'un ensemble d'individus fortement dispersés et individualisés. De même, Juris (2012), à partir du mouvement Occupy, parle de « logique d'agrégation » pour spécifier la manière dont les médias sociaux ont contribué à assembler une masse d'individus aux origines variées au sein d'espaces physiques. Cette conception n'est guère étrangère à Nardi et O'Day qui, déjà en 1999, insistaient sur l'importance de comprendre et explorer les actions des individus par rapport aux technologies dans leur contexte local. Pour ces derniers, les technologies numériques sont le fruit d'une juxtaposition d'un réseau complexe de relations au travers desquelles « only people who are immersed in a particular information ecology can provide a

local habitation and a name to new technologies » (Nardi et O'Day, 1999, cité dans Treré, 2012 : 2364).

1.5. Le salafisme-jihadisme et internet

Cette dernière section aura pour objectif de mettre en lumière le cas à l'étude. Sans déborder les intentions de cette thèse qui consiste à cantonner l'État islamique à une logique de cas, il est toutefois primordial de rendre compte des stratégies de communication mises en place par le groupe au cours de ces dernières années. L'ambition de cette section sera donc de contextualiser la stratégie de visibilité médiatique de l'État islamique. Avant tout chose, il importe d'effectuer un travail sur la mise en agenda de la cause salafiste-jihadiste.

1.5.1. Le salafisme-jihadiste

Le jihadisme tire ses fondements d'une lecture salafiste de l'islam et de la mise en place de stratégies violentes (Maher, 2016 ; Rougier, 2016a ; Thomas, 2016). Cet islamisme, qui se réclame d'un salafisme[18], s'appuie sur un idéologie aux racines anciennes (Migaux, 2015 ; Rougier, 2016a, 2016b). Le salafisme-jihadiste se caractérise entre autres par trois caractéristiques (Brachman, 2009 ; El Difraoui, 2016) : *Al-wala wal-bara'*, le *taghut* et le *takfir*. Le premier concept postule que les musulmans doivent rester loyaux seulement envers les musulmans. Le sens de cette formule est assez fort pour engendrer une dichotomie entre les musulmans et les non-musulmans. Le deuxième concept marque le rapport que doit avoir le musulman à l'idolâtrie. C'est-à-dire qu'il ne peut y avoir d'autres divinités ou saints autres que Dieu. Dans sa forme la plus extrême, toutes obligations ou acceptations qui ne sont pas explicitement indiquées dans le Coran ou la Summa, sont condamnées. Le troisième concept renvoie à l'excommunication des infidèles ou des apostats, et légitimise leur mise à mort.

Le jihadisme est pour sa part au cœur de la croyance religieuse salafiste-jihadiste (Rougier, 2016a). Mais, il existe une forte controverse à savoir qui fait autorité pour prononcer le jihad. Abdallah Azzam a apporté une réponse tranchée à cette indétermination, en indiquant que chaque croyant peut faire son jihad, sans demander une autorisation (Rougier, 2016b). Dès lors, n'importe quel musulman peut prononcer le jihad individuel. Le jihadisme s'établit ainsi

[18] De façon générale, le salafisme envisage de revenir aux sources de la religion et à l'islam originel (Rougier, 2016a). Il prend comme référence les premiers musulmans (les « pieux ancêtres ») et la manière dont ils ont appliqué l'islam dans l'Arabie du 7e siècle. Pour l'auteur il existe trois formes de salafisme : littéraliste, réformiste et jihadiste.

comme une obligation individuelle pour tous les musulmans, et ne concerne plus seulement les populations aux territoires occupés.

L'idéologie jihadiste n'est par ailleurs pas univoque (Hegghammer, 2009 ; Rougier, 2016a ; Roy, 2001). En raison des diverses identités et stratégies adoptées par les jihadistes, le jihadisme se révèle comme étant fragmenté. Hegghammer (2016) identifie deux points de discordes principaux. Le premier concerne l'idéologie. Pour l'auteur, il est important de distinguer l'activisme socio-révolutionnaire, dont le but est de renverser un régime, du nationalisme pan-islamique, qui vise la défense de la *umma*[19]. Au sein de l'activisme socio-révolutionnaire, l'objectif est tourné vers l'intérieur. Il s'agit habituellement de répondre à une oppression interne. Concernant le nationalisme pan-islamique, l'objectif est orienté vers l'extérieur. Il plaide la légitime défense, en raison des agressions extérieures et aux occupations. À ce titre, Ben Laden a émis en 1996 un acte de guerre contre les États-Unis. L'auteur indique qu'au cours de ces dernières décennies, deux types de violences ont été commises par les mouvements jihadistes : des attaques à l'encontre de cibles occidentales et des attaques contre des musulmans qui auraient transgressé des normes.

Deuxièmement, au milieu des années 1990, une rupture a émergé au sein des mouvements jihadistes : le courant jihadiste classique et le courant jihadiste global. Les groupes étaient grandement en désaccord en ce qui concerne l'échelle de l'action (global ou local) et les moyens utilisés. En ce qui concerne les jihadistes classiques, les luttes sont nationales et ils font généralement usage de moyens proches d'une guérilla semi-conventionnelle. Les jihadistes globaux privilégient l'utilisation de tous les moyens et en n'importe quel lieu, dont le terrorisme international. Comme l'auteur l'indique, cette divergence concernant les moyens utilisés a fait l'objet d'une opposition entre Ibn Khattab en Tchétchénie et Ben Laden en Afghanistan.

Pour Khattab, le combat devait uniquement se dérouler sur le sol tchétchène contre des combattants. Ben Laden a préféré privilégier le terrorisme international. L'enjeu pour Ben Laden était de mener une lutte pour la libération. Une lutte qui doit être globale et frapper directement le « cœur des ennemis », comme l'ont fait les attentats du 11 septembre. Les

[19] Dans la terminologie musulmane, la *umma* renvoie à la communauté des croyants. Elle dépasse toute appartenance tribale, ethnique et nationale au profit d'une solidarité entre les membres de la communauté religieuse.

méthodes de combat des jihadistes globaux se sont enrichies d'un moyen qui diffère du jihadisme classique : les attentats suicides. Si ni le terrorisme ni le jihadisme ne sont nouveaux, la quête délibérée de la mort du terroriste est pour sa part novatrice (Roy, 2016). La mort du terroriste n'est plus accidentelle ou le fait d'une circonstance malheureuse, mais délibérée. C'est la finalité par excellence de leur engagement ; c'est la valorisation du martyre suicide (Cook, 2017 ; El Difraoui, 2013, 2016).

1.5.2. La mise en ligne de la visibilité de l'État islamique

De façon générale, la communication jihadiste remplit trois objectifs principaux : le recrutement, la légitimation de la cause et l'intimidation des adversaires (Bockstette, 2009). L'État islamique a rapidement compris l'importance des médias numériques pour rendre sa propagande accessible à n'importe qui et n'importe où. L'ancien dirigeant d'Al-Qaïda en Irak, le jihadiste jordanien Abou Moussad al-Zarqaoui, a ainsi très tôt vanté les mérites d'une diffusion sur internet des vidéos des atrocités commises par l'organisation (El Difraoui, 2013, 2016). L'État islamique a par la suite développé une visibilité efficace reposant sur des pratiques de production centralisées combinées à des stratégies de diffusion décentralisées (Mahlouly et Winter, 2018 ; Lorenzo-Dus et Macdonald, 2019 ; Saltman et Winter, 2014 ; Winter, 2015 ; Zelin, 2015). Ce succès est dû au fait que l'organisation a misé autant sur la qualité que sur la quantité des contenus offerts à des audiences mondialisées.

Il est aujourd'hui communément admis que l'État islamique est largement présent au sein des médias sociaux (Awan, 2017 ; Blaker, 2015 ; Bloom et al., 2019 ; Ceron et al., 2018 ; Farwell, 2014 ; Gates and al., 2015 ; Huey et al., 2017 ; Klausen, 2015 ; Piazza et Guler, 2019 ; Richards, 2016 ; Winter, 2015). Les militants sont présents sur les principaux réseaux sociaux, comme Facebook, YouTube et Twitter, ainsi que sur des messageries cryptées plus difficiles à contrôler, telles que WhatsApp et Telegram. Twitter a été pendant longtemps l'une de ses plateformes de prédilection. Selon une étude menée par Berger et Morgan (2015), le nombre de comptes Twitter reliés à l'État islamique était estimé à plus de 46 000 en 2014.

Ces applications web ont comme propriété de rendre plus visible que jamais leur propagande aux partisans, adversaires et journalistes (Farwell, 2014). Elles sont devenues le canal privilégié pour diffuser des images puissantes et émotionnelles. Mahlouly et Winter (2018) ont noté que cinq thématiques ressortaient particulièrement de la propagande de l'État islamique : la brutalité, la miséricorde, l'appartenance, la victimisation, la guerre et l'utopie.

Ces thématiques pourront être consommées dans différents formats qui comprennent par exemple des revues (Ingram, 2016 ; Wignell et al., 2017), vidéos (Chouliaraki et Kissas, 2018), infographies (Adelman, 2018) et images (Kraidy, 2017).

Si l'État islamique a semblé novateur dans ses stratégies de communication, El Difraoui (2016) rappelle combien la guerre médiatique de l'État islamique s'est bâtie sur un Grand Récit jihadiste développé depuis plus de trente ans. Al-Qaïda est l'une des premières mouvances à avoir utilisé l'audiovisuel comme principal support de diffusion de leur propagande (El Difraoui, 2003)[20]. Les premières vidéos auraient été produites en 1998. L'époque des grandes mises en scène médiatique allait battre son plein, en cherchant à susciter des « vocations d'apprentis kamikaze » (El Difraoui, 2003 : 13). Parallèlement, dès les années 2000, internet a commencé à jouer un rôle considérable dans les communications des mouvements salafistes-jihadistes (Awan, 2007b ; Bockstette, 2009 ; Rudner, 2017 ; Thomas, 2016). Cette mise en circulation d'informations salafistes-jihadistes sur internet a donné lieu à des appellations de type « jihad électronique » (Rudner, 2017), « jihad virtuel » (Corman et al., 2006) et plus récemment, « califat virtuel » (Winter, 2015).

Avec l'avènement d'internet, la formation des militants, les martyres et l'idéologie allaient maintenant être systématiquement enregistrés, filmés et propagés à une audience mondialisée (Thomas, 2016). Internet allait également leur offrir la possibilité d'archiver et numériser des prêches salafistes et jihadistes, populaires auprès des militants. Les plus ambitieux pouvaient quant à eux développer des logiciels spécialisés ou des programmes qui préservent leurs données personnelles. Au-delà de ces activités, l'auteur rappelle qu'ils investissent aussi un temps important à émettre des consignes électroniques et à exploiter des systèmes cryptographiques.

L'activisme jihadiste en ligne doit toutefois son essor à la guerre en Irak (El Difraoui, 2016, Thomas, 2016). Internet a largement été utilisé lors du conflit. Se diffusaient sur internet des communiqués de mouvements jihadistes, des bulletins d'information ou encore des revues jihadistes. Les jihadistes échangeaient pour leur part des informations, opinions, photos ou vidéos sur les mouvements jihadistes et la guerre. Thomas (2016) indique que les forums

[20] Il existe des précédents à la propagande audiovisuelle d'Al-Qaïda (El Difraoui, 2003, 2016). Lors de la guerre d'Afghanistan contre l'Union soviétique a émergé des films mettant en scène le culte du martyre, théorisé par Abdallah Azzam. Une autre phase majeure dans l'essor de la propagande audiovisuelle est la guerre en Bosnie. Cette phase a été marquée par une professionnalisation des vidéos, qui leur a permis de sortir des cercles jihadistes et de toucher une audience musulmane plus large.

jihadistes étaient régulièrement composés des mêmes rubriques : général, actualités jihadistes, vidéos et sons, communiqués, technologies, entraînement. Les activités en ligne des salafistes-jihadistes sont ainsi larges et multiples. Elles comprennent : la diffusion d'information, de la propagande, de directives opérationnelles, de formations, ainsi que le recrutement ou encore la création d'une communauté en ligne (Bockstette, 2009 ; Gill et al., 2017 ; Rudner, 2017 ; Torres, 2010 ; Torres et al., 2006). Internet a donc modifié le paysage communicationnel des mouvements salafistes-jihadistes (El Difroui, 2016). Alors que la propagande jihadiste était majoritairement produite localement par des groupes jihadistes, internet a ouvert la voie à une diffusion à travers le monde entier par des regroupements informels de sympathisants.

C'est aussi au moment de la guerre d'Irak que plusieurs genres de vidéos se sont déployés. El Difraoui en identifie cinq. La première catégorie est celle des vidéos d'entraînement, de formation et d'assaut qui ont pour vocation de recruter de nouveaux jihadistes. La deuxième concerne les vidéos de menaces, d'otages et d'exécutions. Elles cherchent à mener une guerre psychologique en terrorisant « le cœur des ennemis ». Les vidéos qui font l'éloge des martyres constituent un troisième type. Le but est de convaincre des jeunes militants d'accomplir des attentats suicides, afin d'atteindre le paradis. Un quatrième genre est celui du *jihad-pop*, primordial pour attirer la jeunesse occidentale à rejoindre le jihad global. Il s'agit de superposer des contenus jihadistes à la culture occidentale. Le dernier genre de vidéo se rapporte à des vidéos didactiques, qui rassemblent un ensemble d'éléments divers. Elles ont pour rôle de convaincre par des moyens didactiques, idéologiques et émotionnels du bien-fondé du jihad et du martyre.

Si Al-Qaïda a posé les bases de l'écosystème médiatique des jihadistes, l'État islamique l'a profondément élargi et perfectionné (Dauber et Robinson, 2015). À mesure que l'État islamique évoluait, les propagandistes ont rapidement surpassé leurs rivaux d'Al-Qaïda en misant sur l'innovation et la sophistication (Burke, 2016 ; Koerner 2016 ; Winter, 2018). Grâce au recrutement d'une nouvelle génération de jihadistes très avertis des nouvelles technologies, l'organisation a pu exploiter massivement un nouvel arsenal (caméras digitales, ordinateurs portables, téléphones intelligents, médias sociaux et messageries cryptées) aussi bien à l'intérieur qu'à l'extérieur de ses zones d'opération.

Outre ce professionnalisme, elle a également réussi à accroître son influence en réinterprétant les opérations médiatiques des groupes salafistes-jihadistes, comme en témoigne son

document *Media Operative, You are a Mujihad, Too*, diffusé en avril 2016 en langue arabe sur ses chaînes Telegram officielles. Contrairement à d'autres organisations salafistes-jihadistes, l'État islamique a institué une certaine flexibilité d'action en maintenant délibérément le flou entre les centres médiatiques rattachés officiellement à l'État islamique et les activistes autoproclamés. Cela lui a permis de paraître moins hiérarchique, donc d'être plus attrayant, tout en déléguant à une plus grande masse d'individus le soin d'accroître la portée de ses messages sur les médias sociaux et les messageries cryptées. Différents types d'utilisateurs opèrent ainsi en ligne : sympathisants, propagandistes, combattants, recruteurs et adversaires (Magdy et al., 2015). Aussi, au contraire d'Al-Qaïda, l'État islamique a misé sur des répertoires audiovisuels plus polyvalents, souples et percutants ; combinant ultra-violence et bonne gouvernance (Byman, 2016).

Cette forte présence de l'organisation sur les réseaux sociaux numériques a rapidement inquiété les pouvoirs publics. La présence accrue de l'État islamique a renouvelé la question de la régulation des médias sociaux (Crosset et Dupont, 2018). Cette régulation représente des défis dans la mesure où elle fait intervenir une pluralité d'acteurs qui mobilisent à des politiques étatiques interventionnistes, des politiques de *laisser-faire* propres aux entreprises de la Silicon Valley ou encore des formes participatives de régulation par le bas. Nous avons montré que contrer la régulation de la propagande jihadiste dépend d'un ensemble d'acteurs issus du secteur public, du secteur privé et de la société civile. Ces acteurs allient principalement trois types d'activités : l'exclusion des jihadistes des réseaux sociaux, à la discrétion des plateformes numériques ; la circulation de contre-discours par la société civile, des associations et des gouvernements ; la mise en place de dénonciations et signalements de comptes jihadistes effectués par des cyber-vigilants et des collectifs d'hacktivistes.

Conclusion

Cette revue de la littérature nous mène à trois constats majeurs. Premièrement, la visibilité des groupes activistes est primordiale. Les études en sociologie des mouvements sociaux ont montré que les groupes protestataires produisent de nombreux discours qu'ils rendront visibles par le biais de diverses technologies de communication. De plus, les groupes protestataires développeront des stratégies de visibilité, parfois très spécifiques. C'est le cas par exemple des groupes extrémistes qui privilégient une propagande par le fait et le choc émotionnel.

Deuxièmement, la recherche montre que la visibilité s'accompagne de luttes pour accéder à l'espace d'apparence. Cela découle, entre autres, d'une particularité spécifique à cet espace : il s'agit d'un lieu où s'entrecroisent des luttes de légitimation et de disqualification entre les acteurs qui y participent. En cela, l'espace d'apparence est intrinsèquement conflictuel, asymétrique, pluriel et plastique. Plus spécifiquement, en ce qui concerne les mouvements sociaux, la recherche a montré que leur visibilité fait l'objet de luttes multiples entre l'État, les intermédiaires et les adversaires. À cet effet, les militants peuvent être victimes de censure ou alors de contre-cadrages qui visent à les décrédibiliser.

Troisièmement, il existe un consensus au sein de la recherche sur le fait que les activistes disposent maintenant de technologies numériques pour rendre visible leur cause à une large audience. Toutefois, la recherche sur l'activisme en ligne, et plus généralement, les technologies de communication, ont rarement pensé l'activité au-delà du dualisme humain/technique. Plutôt, la recherche a privilégié une tendance fonctionnaliste et instrumentalise des descriptions du phénomène. Ce faisant, la question des possibilités de co-constitution entre militants et technologies a totalement été exclue. De plus, peu d'études ont pris en considération le rôle des non-humains dans le fonctionnement de la visibilité des militants. Dit autrement, les couches techniques des technologies de communication sont souvent passées sous silence. Cela nous appelle à penser la visibilité des activistes au-delà des dualismes traditionnels (humain/technique, anciens/nouveaux médias, hors ligne/en ligne) ; ainsi qu'à prendre au sérieux le rôle de la matérialité dans la structuration de la participation en ligne. Ces différents constats nous autorisent à restituer la visibilité de groupes militants dans toute la complexité qu'elle dissimule. Toutefois, maintenant que nous avons identifié les contours de cette complexité, il nous faut affiner notre angle d'approche en portant notre attention sur les technologies du web.

Chapitre 2 : Être visible sur le web. La mise en ligne de la contestation

Jusqu'à présent nous avons porté notre attention aux dynamiques de visibilité liées aux technologies de communication et à l'usage que pouvaient faire les activistes des plateformes numériques. Reste à savoir comment cette visibilité s'inscrit et circule au sein de ces technologies numériques. Pour cela, notre recension des écrits doit se pencher sur les spécificités d'internet en tant que sphère d'apparence, les fondations techniques et politiques de ces technologies numériques et les contraintes liées à la modération. Pour y voir plus clair, nous proposons de procéder en quatre temps. La première section sera consacrée à la recension des différents débats sur le rôle d'internet dans la transformation de l'espace public, qui nous poussera à poser le constat d'une littérature fragmentée. La deuxième partie s'intéressera à la manière dont les architectures techniques formatent différents modèles de visibilité. Dans la troisième section, nous aborderons les spécificités techniques de ces architectures, en décrivant les différentes couches qui les composent. Nous porterons notre attention sur le code, les algorithmes, les données et les protocoles. Enfin, partant du principe que les pratiques de visibilités ne doivent pas être isolées d'autres ressources de types organisationnels, la section portera aussi sur l'exercice de la modération en ligne et sur la contrainte qu'elle impose aux flux informationnels. L'ensemble de ce chapitre nous permettra de préciser notre compréhension des dynamiques techniques et politiques sous-jacentes aux technologies numériques et à l'espace d'apparence qu'elles ouvrent.

2.1. Avènement du web 2.0 : Un nouvel espace émancipateur ?

Notre recherche s'intéresse à la visibilité de groupes qualifiés d'extrémistes dans un contexte spécifique : le web 2.0. Comme toutes technologies de communication dans le passé, le web 2.0 a d'abord été célébré dans sa dimension émancipatrice, pour ensuite être nuancé par une évaluation plus mesurée (Loader et Mercea 2011). Avant de nous intéresser aux nombreux débats sur le potentiel émancipateur d'internet qui ont eu lieu ces dernières années, nous commencerons par rendre compte des caractéristiques du web 2.0 comme plateforme numérique.

2.1.1. Le web 2.0 comme plateforme

À la suite de l'éclatement de la bulle spéculative d'internet au début des années 2000, une nouvelle mutation allait se produire, celle qu'on a pris l'habitude de nommer le web 2.0 après sa popularisation par Tim O'Reilly en 2005. Dans la conception poreuse qu'en donne O'Reilly, le web englobe à peu près tout : réseaux sociaux numériques, initiatives open source comme Wikipedia ou encore des plateformes de commerce électronique telles qu'Amazon. Pour O'Reilly et Battelle (2004), le web est maintenant « a robust development environment » au travers duquel « websites become software components ». Plus qu'un nouveau type de web, Allen (2013) estime qu'il est préférable d'entrevoir le web 2.0 comme une « technologie rhétorique », « through which the computing industry attempted to change the way we think of the internet » (p.264). Pour l'auteur, ce concept marketing permettait de prétendre à la nouveauté d'un produit et de relancer un marché sur des bases sensiblement différentes. Il ne s'agissait plus de transposer des modèles économiques traditionnels dans le numérique, mais de placer cette fois-ci en premier lieu les dynamiques d'usage (Cardon, 2019).

L'une des principales particularités de l'ensemble des applications web qui se sont multipliées aux abords des années 2005 est d'avoir placé les usagers au centre du dispositif. Effectivement, ces sites web se structurent avant tout à partir d'un grand nombre d'utilisateurs qui endossent un rôle de producteur-utilisateur de contenus médiatiques (Beer et Burrows, 2007 ; Benkler, 2009 ; Proulx, 2011 ; Proulx, Milette et Heaton, 2011). Cela se base sur l'idéologie du web social, à savoir que « les gens ordinaires - les amateurs, les citoyens, les utilisateurs *lambda* - en viennent à développer une compétence cognitive et communicationnelle suffisante pour leur permettre d'intervenir directement dans la

production et la diffusion de contenus médiatiques, qu'il s'agisse d'information, de recommandations culturelles ou de publicité » (Proulx et al., 2011 : 3).

Si les nouveaux services web ont permis de simplifier l'autonomie des internautes, en termes d'auto-publication, de présentation de soi et de collaboration, c'est notamment en raison d'une architecture plus conviviale et participative (Boullier, 2016 ; Langlois et al., 2009a). Par le biais de processus techniques complexes, ces nouveaux services web ont misé sur l'accès à des modèles de publication préétablis à partir desquels l'utilisateur sera en mesure de publier du contenu sans avoir à écrire une ligne de code. Ainsi, « les sites web que l'on publiait auparavant en HTLM directement et qui demandaient donc de manipuler du code ont été équipés par des bases de données qui permettent de transformer tout ce qui est publié en HTLM » (Boullier, 2016 : 81).

Ces usages et activités sont toutefois de plus en plus cooptés par un ensemble de plateformes numériques. Le vocable de plateforme a été assigné au web 2.0 dès ses débuts. C'est au moment de la première conférence web 2.0 en 2014, que Tim O'Reilly et John Battelle ont évoqué ce principe devenu largement répandu : « the web as plateform ». Après cela, le web 2.0 a régulièrement été désigné comme « web-as-participation-plateform » et le web 1.0 comme « web-as-information-source » [21] (Song, 2010). Gillespie (2010) estime que l'utilisation de la notion de plateforme révèle avant tout un travail discursif permettant d'interpeller une vaste gamme d'acteurs hétérogènes : « the term has been deployed in both their populist appeals and their marketing pitches, sometimes as technical 'platforms', sometimes as 'platforms' from which to speak, sometimes as 'platforms' of opportunity » (p.347).

L'usage flexible et polysémique de la notion impute à ces acteurs un positionnement hautement stratégique, essentiel à leur profit. L'auteur fait valoir que ce terme s'articule autour de quatre signifiés majeurs : un sens computationnel d'infrastructure qui construit des

[21] En réalité, la ligne de démarcation entre le web 1.0 et le web 2.0 est moins évidente qu'elle n'y paraît (Allen, 2013 ; Cormode et Krishnamurthy, 2008 ; Song, 2010). Les usages associés au web 2.0 étaient manifestes dans les activités en ligne qui le précédaient (Allen, 2013). L'auteur indique que durant les années 1990 de nombreux internautes souhaitaient partager des informations, créer du contenu et interagir avec les autres. Cela s'est traduit par plusieurs canaux de distribution en réseau comme Usenet, les babillards électroniques, les listes de courrier électronique, les environnements de discussion en ligne et les domaines multi-utilisateurs. La littérature tend néanmoins à affirmer qu'internet qu'on connaît aujourd'hui est à maints égards différent de celui des années 1990. Les tendances actuelles des grands réseaux sociaux, tels que Facebook, n'ont plus grand-chose à voir avec les « communautés en ligne » du milieu des années 1990.

applications ; un sens physique et architectural à travers lequel des personnes ou des objets peuvent se tenir pour exercer une activité particulière ; un sens figuratif comme la fondation et le fondement de possibilités, d'actions et de réalisations futures ; un sens politique qui décrit un programme d'action. Pris ensemble, le terme de plateforme « emerges not simply as indicating a functional shape: it suggests a progressive and egalitarian arrangement, promising to support those who stand upon it » (Gillespie, 2010 : 350).

Cet écosystème de plateformes numériques est aujourd'hui principalement dominé par cinq entreprises américaines (Google, Apple, Facebook, Amazon et Microsoft) rassemblées au sein de la Silicon Valley. Cet oligopole impose dans une certaine mesure une conception globale de l'ensemble du réseau et de la distribution des flux de données (Gehl, 2014 ; van Dijck, Pell et de Wall, 2018). Le fait qu'il y ait une domination de certaines plateformes n'est pas une coïncidence historique, mais est la conséquence de deux dynamiques structurelles importantes : « the network effects[22] and the dominance of the ad-financing model for online platforms » (Tufekci, 2017 : 135).

Les milliards d'utilisateurs qui utilisent internet sont par conséquent capturés par un petit nombre d'entreprises qui configurent leur activité (Tufekci, 2017). À titre d'exemple, van Dijck et ses collaborateurs (2018) indiquent qu'à côté de Google, Facebook contrôle 80 % du marché des services de réseaux sociaux, avec plus de deux milliards d'utilisateurs mensuels dans le monde. Cornant la concurrence, ces entreprises dominantes surveillent les entrepreneurs de nouvelles plateformes numériques à fort potentiel de croissance pour racheter ou incorporer leurs découvertes dans leurs propres produits (Fligstein, 2001 ; Langlois et al., 2009a ; Proulx, 2015a). Google a par exemple acheté YouTube pour 1,65 milliard en 2006. Facebook est également connu pour acquérir des jeunes entreprises afin de maintenir sa position d'acteurs majeurs, comme cela a été le cas avec le rachat d'Instagram (2012) et de WhatsApp (2014). En achetant ces applications, auxquelles il faut ajouter Messenger, Facebook a considérablement renforcé sa puissance de collecte de données personnelles.

[22] Comme l'auteure l'explique, le terme « effets de réseaux » (ou « *network externalities* ») encapsule le principe que plus des personnes utilisent la plateforme, plus la plateforme sera utile pour chacun des utilisateurs. Cet effet est particulièrement fort en ce qui concerne les plateformes des médias sociaux.

Van Dijck et ses collaborateurs rappellent que la publicité en ligne est quant à elle contrôlée à plus de 60 % par Facebook et Google. Face au fort potentiel économique de ces entreprises, elles tiennent une position dominante en matière de chiffres d'affaires et s'insèrent dans le rang des plus grandes entreprises américaines. Le dernier classement des entreprises américaines publié en 2019 par le magazine *Fortune*, révèle par exemple que le chiffre d'affaire d'Apple avoisine les 265,6 milliards de dollars, ce qui la place en troisième position du classement après Walmart et Exxon Mobil. Quant à leur capitalisation boursière, les entreprises high-tech occupent les premières places du classement. Ce faisant, ce qui domine le web 2.0, ce sont des modèles d'affaires à la fois ambitieux et agressifs (Langlois et al., 2009a).

La manière dont ces plateformes créent et capturent de la valeur se fait au travers de différents procédés spécifiques au web. Van Dijck et ses collaborateurs indiquent à ce titre que « along with money and attention, data and user valuation have become popular means of monetization » (2018 : 5). La monétisation des grandes plateformes numériques s'effectue ainsi grâce à une automatisation des connexions entre les utilisateurs, le contenu, les données et la publicité (Couldry, 2015 ; van Dijck et al., 2018). La logique à l'œuvre n'est donc pas la gratuité en tant que telle, mais un échange de données personnelles contre des services particuliers (Schneirer, 2015).

Dès lors, cette *plateformization* du web[23] (Helmond, 2015) s'inscrit dans des structures qui se veulent à la fois économiques, politiques et culturelles (Couldry, 2015 ; Fuchs, 2014 ; Srnicek, 2017 ; Turow, 2012). On comprend plus facilement que ces services se basent sur des modèles techniques et économiques pour établir une architecture plutôt qu'une autre, ainsi qu'une norme au détriment d'une autre (Lessig, 2006). Sur le plan technique, il s'agit pour ces différents services de valoriser un modèle de centralisation et d'architecture de type client-serveur (Boullier, 2012). Cette anatomie repose sur un protocole simple où le client demande un service à un serveur qui stocke des données et des informations et/ou gère le trafic (Musiani, 2013). Le client est ici la machine qui donne un accès à l'utilisateur aux données stockées sur un serveur à distance. La puissance économique des compagnies de services technologiques dépend ainsi de la capacité de ses serveurs à stocker des données massives, à s'y connecter et à analyser les données (Boullier 2012 ; Hogan 2015). Cette centralisation lui

[23] Helmond (2015) définit le phénomène de *platformization* comme « rise of the platform as the dominant infrastructural and economic model of the social web and its consequences » (p.1).

assurera au bout du compte une propriété et un contrôle technique absolus sur les informations stockées au sein de puissants serveurs[24].

Cette *plateformization* du web dévoile par conséquent trois effets majeurs sur l'écosystème numérique (Boullier, 2016). Premièrement, une centralisation du réseau et de son trafic qui s'écarte de l'internet distribué de ses débuts. Deuxièmement, des espaces de plus en plus clos, qui n'ont plus grand-chose à voir avec le principe de générativité décrit par Zittrain (2008). Enfin, un monopole absolu sur les données et les traces produites par les usagers. Ainsi, pour reprendre l'argumentation de van Dijck et ses collaborateurs, nous pouvons dire que dans le contexte actuel où le web 2.0 est dominé par des oligopoles une série de paradoxes peuvent être soulignés :

> It [the platform ecosystem] looks egalitarian yet is hierarchical; it is almost entirely corporate, but it appears to serve public value; it seems neutral and agnostic, but its architecture carries a particular set of ideological values; its effects appear local, while its scope and impact are global; it appears to replace "top-down" "big government" with "bottom-up" "customer empowerment" yet it is doing so by means of a highly centralized structure which remains opaque to its users. (2018 :8).

2.1.1. L'idéal d'un nouvel espace public

Manifestement, internet et démocratie sont devenus des termes intimement liés : l'utopisme technologique a rapidement célébré sans discernement le rôle d'internet dans les processus démocratiques et de transformation de l'espace public (Benkler, 2009 ; Burgess et Green, 2009 ; Castells, 2009 ; Hauben et Hauben, 1998 ; Jenkins, 2006 ; Kahn et Kellner, 2004 ; Leadbeater, 2008 ; Papacharissi, 2002 ; Rheingold, 1993). Dès le début des années 1990, internet a souvent été dépeint comme une nouvelle « agora électronique » (Flichy, 2008a). Le fait qu'une technologie qui élargit la visibilité soit considérée comme révélatrice d'un nouvel espace public n'est pas quelque chose de nouveau en soi (Couldry, 2015 ; Cardon, 2019). Cela avait déjà été le cas avec la presse, la radio et la télévision qui renvoie régulièrement à un espace public dit traditionnel. Si cet espace de visibilité est réputé pour exercer un filtrage de l'information par des *gatekeepers*, il n'est pas étonnant que l'utopie relative aux effets

[24] Cette assertion nécessite néanmoins d'être nuancée, puisque certains services Cloud assurent que la propriété des données reste celle des clients. Voir par exemple Google Cloud https://cloud.google.com/security/privacy/?hl=fr

émancipateurs d'internet ait été l'un des plus grands éléments d'attraction de cette nouvelle technologie.

Sans examiner toutes les références en la matière, nous centrerons notre attention sur deux moments clés de la rhétorique utopiste générée par l'accélération des technologies numériques (Loader et Mercea, 2011). À ses débuts, la discussion concernant le potentiel démocratique d'internet a habituellement reposé sur la sphère publique délibérative théorisée par Habermas (voir par exemple Brundidge, 2010 ; Chambers et Costain, 2000 ; Dahlberg, 2007 ; Gimmler, 2001 ; Shane, 2004 ; Witschge, 2004). Dans sa formulation originale, Habermas (1989) fait de l'espace public le lieu d'un débat ouvert, raisonné et réflexif sur des questions d'intérêts communs. La production et la circulation de ce flux d'informations et d'idées s'exercent par l'entremise de rencontres face à face et en interactions médiatisées. Présentée comme un idéal type, la grammaire substantive de l'espace public impose qu'elle réponde à un principe d'émancipation. Les partisans de la démocratie délibérative comprennent ainsi internet comme un moyen privilégié pour la mise en œuvre d'un tel espace dialogique (Dahlberg, 2001 ; Loader et Mercea, 2011). Ces auteurs ont supposé qu'internet serait la réalisation par excellence d'une démocratie plus participative, où s'exercerait partiellement ou totalement un dialogue rationnel-critique.

Loader et Mercea (2011) expliquent qu'une nouvelle vague d'optimisme est récemment apparue avec l'avènement des plateformes des réseaux sociaux telles que Twitter, Facebook, YouTube, les wikis et la blogosphère. Ce discours repose cette fois-ci sur le postulat d'une démocratie en réseau centrée sur le citoyen-utilisateur. Cela fait surgir un écart par rapport aux idéaux d'une délibération rationnelle qui considère avant tout les citoyens comme des êtres consciencieux et avertis. Plutôt, ces nouvelles affirmations enthousiastes assimilent les réseaux sociaux à une forme d'organisation sociale plus horizontale. Par exemple, Rainie et Wellman (2012) suggèrent que les médias sociaux caractérisent ce qu'ils nomment un « individualisme en réseau », en contraste à des organisations sociales formées autour de grandes bureaucraties hiérarchiques ou encore de petits groupes comme les ménages, les communautés, les groupes de travail, etc.

Les auteurs comparent l'individualisme en réseau à un système d'exploitation, car il dépeint les façons dont les gens se connectent, communiquent et échangent des informations. L'expression souligne le fait que les systèmes informatiques ont des structures en réseau qui

offrent un ensemble de possibilités, de contraintes, de règle et de procédures. Comme tout système informatique ou système mobile, le système d'exploitation de cette structure réseautique est personnel (l'individu est un centre autonome, à partir de son ordinateur) ; multi-utilisateur (les gens interagissent avec d'autres internautes) ; multi-tâche (les usagers peuvent effectuer de nombreuses tâches) ; multi-simultané (il réalise de multiples tâches simultanées).

Pour le sociologue Manuel Castells (2009), nous nous trouvons dans un « new world of mass self-communication »[25] (p.417) qui chamboule la sphère publique par ses capacités d'autonomisation et de partage en masse de messages multimédias. L'auteur conçoit que ce nouveau système de communication qui vient concurrencer, contredire, mais aussi nourrir les grands médias se singularise par sa flexibilité, sa diversité et son caractère évolutif. En cela, « it integrates messages and codes from all sources, enclosing most of socialized communication in its multimodal, multichannel networks » (p.417). Dans son modèle, Castells fera de l'auto-communication de masse un droit à faire prévaloir afin que tout citoyen puisse garder une autonomie. Cela passe notamment par le fait de préserver une liberté et une équité dans le déploiement et la gestion de l'infrastructure de communication en réseau et des industries des médias, car « liberty, and ultimately social change, become entwined with the institutional and organizational operation of communication networks » (Castells, 2009 : 302-302).

Benkler (2009), dans son éminent ouvrage la *Richesse des réseaux,* souligne quant à lui l'émergence d'un nouvel espace public en réseau. Ce dernier a mis de l'avant que les nouveaux modes de production hors marché par des producteurs indépendants ont une influence notoire sur nos modes de production et de consommation de l'information. Les nouvelles technologies de l'information et de la communication ont ainsi participé à créer une « économie de l'information en réseau » et ont supplanté « l'économie industrielle de l'information du vingtième siècle » (Benkler, 2009 : 30). L'auteur rappelle qu'au contraire des médias de masse qui sont bâtis à partir d'une architecture en étoile qui comprend des liens

[25] L'auteur définit cette « auto-communication de masse » de la façon suivante : « It is mass communication because it can potentially reach a global audience, as in the posting of a video on YouTube, a blog with RSS links to a number of web sources, or a message to a massive e-mail list. At the same time, it is self-communication because the production of the message is self-generated the definition of the potential receiver(s) is self-directed, and the retrieval of specific messages or content from the World Wide Web and electronic communications networks is self-selected » (2009 : 55).

unidirectionnels avec l'émetteur, internet se caractérise par une architecture distribuée qui se compose de liens multidirectionnels entre tous les nœuds du réseau.

L'architecture en réseau et la réduction des coûts de l'accessibilité à la communication ont ainsi « fondamentalement modifié la capacité des individus, agissants seuls ou en groupe, à être d'actifs participants à l'espace public, par opposition à ses lecteurs, ses auditeurs et téléspectateurs passifs » (p.275). En cela, pour l'auteur, internet permet « un glissement d'un espace public mass-médiatique vers un espace public en réseau » (p.39). Les changements liés au paysage médiatique incitent Henry Jenkins (2006) à parler de « culture participative » pour signifier ces nouvelles formes culturelles où les individus participent activement à la création et à la circulation de nouveaux contenus. Il présage que ces nouveaux régimes médiatiques, liés aux nouvelles technologies de l'information et de la communication, favorisent grandement les relations et les collaborations entre les individus pour atteindre une connaissance globale d'un phénomène.

Les auteurs évoqués ci-dessus sont certes différents sur la façon dont ils conceptualisent le réseau, la nouveauté et la culture, mais non sans rapport : on peut dire que chacun d'entre eux problématise la manière dont internet est venu incarner un espace libre d'expression horizontal et en réseau. Cette évolution narrative est celle d'un « époqualisme » (Morozov, 2014) qui envisage internet comme un artefact technique à la fois unique et stable, significatif de nouvelles formes d'auto-détermination et de décentralisation. Hélas, on voit bien la circularité problématique de ces discours utopistes qui négligent la matérialité et les modèles d'affaires propres à la plupart des grands services de réseaux sociaux qui capturent davantage ces espaces d'expression (Fuchs, 2014). Nous verrons dans ce qui suit que d'autres chercheurs contestent l'hypothèse de l'émergence d'un nouvel espace public en ligne. Ces critiques ne nient pas l'importance de l'avènement des technologies numériques et de leur rôle dans la démocratisation de la consommation et la production de l'information, toutefois elles émettent un discours plus nuancé sur les effets émancipateurs de ces dernières.

2.1.2. Homogénéité des opinions et auto-convictions

Comme nous le développerons dans le chapitre 2, ce qui distingue internet des précédents médias s'inscrit dans sa capacité à offrir aux internautes une information personnalisée en tirant profit de ses algorithmes de recommandation. Ce filtrage automatisé renforce ainsi

l'idée qu'internet devient un agrégateur d'intérêts individuels (Flichy, 2008a). Si ces filtres automatisés sont conçus pour aider l'utilisateur à s'orienter dans la masse d'information, ils le sont également pour favoriser leur engagement sur la plateforme dans le but de vendre leurs traces d'activité et données personnelles aux annonceurs (Cardon, 2019 ; Pariser, 2011 ; Vaidhyanathan, 2018). Pour certains commentateurs, ces filtres automatisés conduiraient à des formes d'isolement idéologique et à la polarisation du débat en ligne. Cette critique renvoie au concept plus connu de « bulle de filtres » popularisé par Pariser (2011). L'auteur estime qu'en proposant des informations en conformité avec nos goûts et nos orientations politiques, les algorithmes renforcent nos tendances naturelles à l'homophilie des opinions.

En considérant qu'internet amplifie l'évitement à des opinions divergentes, il peut être aisé d'y voir une atteinte au bon déroulement du débat démocratique en ligne. Le EU High Level Group on Media Freedom and Pluralism indique à cet égard : « Increasing filtering mechanisms makes it more likely for people to only get news on subjects they are interested in, and with the perspective they identify with. Such developments undoubtedly have a potentially negative impact on democracy » (Vīķe-Freiberga, 2013 : 27). Plusieurs chercheurs ont cependant nuancé cette vision. Helberger et ses collaborateurs (2018) rappellent par exemple que « filtering and recommender systems are not all the same and their impact is not inevitable or beyond human control » (p.192). Cela s'exprime par le fait que les usages et les activités en ligne des internautes influencent les algorithmes (Cardon, 2015 ; Helberger, 2015 ; Helberger et al., 2018 ; Nguyen et al., 2014). Cardon (2015) précise cette position en expliquant que lorsqu'un internaute présente à l'algorithme un usage singulier, original ou périphérique, les recommandations produites ne l'exposeront pas vers des informations et des personnes aux goûts similaires et conformes.

Si les débats autour du cloisonnement des espaces de débats en ligne ont trouvé une nouvelle actualité avec les algorithmes de recommandation, ils ne sont toutefois pas récents. Depuis qu'internet a commencé à être diffusé au sein du grand public, plusieurs auteurs (voir par exemple Graham, 1999 ; Hill et Hughes, 1998 ; Selnow, 1998 ; Sunstein, 2007 ; Shapiro, 1999) ont dénoncé le potentiel de chambres d'écho auquel nous renvoie internet. Cet avertissement d'un risque d'une « balkanisation des opinions » (Flichy, 2008a) a trouvé un grand retentissement avec le livre *Republic.com* du juriste américain Cass Sustein (2007). Dans son ouvrage, l'auteur revient largement sur la façon dont internet fragmente l'espace public en une série d'« enclaves délibératives » où des groupes délibèrent de façons plus ou

moins isolées. À force de réunir essentiellement des internautes d'opinion proches, internet favoriserait à terme la polarisation de groupes aux positions extrêmes.

D'autres recherches contestent néanmoins cet argument jugé peu étayé empiriquement (voir Helberger, 2015 ; Nguyen et al., 2014 ; Stromer-Galley, 2002). Ces études soutiennent l'idée que tout en permettant aux internautes de trouver des groupes aux intérêts identiques, internet offre une diversité informationnelle inégalable dans d'autres contextes. Par exemple, l'étude d'Horrigan (2001) constate que sur 1 697 utilisateurs américains interrogés, 50 % indiquent qu'internet leur a permis de mieux connaître des personnes qu'ils n'auraient pas rencontrées hors-ligne. L'étude de Muhlberger (2004) sur la fragmentation politique en ligne a quant à elle conclu que les débats en ligne ne sont pas plus polarisés que ceux menés dans le monde physique. Selon les résultats de l'étude, elle est même légèrement inférieure à celle hors-ligne.

Horrigan et ses collaborateurs (2004) ont pour leur part démontré que lors de la période qui a précédé l'élection présidentielle américaine de 2004, internet a joué un rôle important dans la prise de conscience d'opinions politiques divergentes. Leur étude note par exemple que les internautes ont été confrontés à une série d'arguments remettant en question leurs opinions contrairement aux personnes qui ne faisaient pas d'internet un usage quotidien. Ceux-ci soutiennent dès lors que « while all people like to see arguments that support their beliefs, internet users are not limiting their information exposure to views that buttress their opinions » (2004 : i-ii). L'enquête récente de Dubois et de Blank (2018) menée auprès de 2 000 internautes adultes au Royaume-Uni ajoute par ailleurs que les internautes qui ont tendance à éviter les chambres d'écho sont ceux qui avaient déjà un intérêt marqué pour la politique et qui avaient pour habitude de consulter des sources médiatiques variées.

Cet enjeu de la polarisation des débats en ligne est intéressant dans la mesure où il permet de montrer la réelle ambiguïté de l'idée d'une sphère publique en ligne qui serait délibérative. Néanmoins, ces positions fragmentées se rejoignent paradoxalement sur un point : celui de perpétuer l'opposition binaire du réel et du virtuel. Au sein de ces différentes perspectives, le débat politique en ligne serait désincarné du monde réel. Ces perspectives sont dès lors dans l'impossibilité de saisir les possibilités de co-influences entre ces différents mondes.

2.1.3. La concentration de l'information

Sans conteste, l'information en ligne est quantitativement très importante (Flichy, 2008a). L'absence de *gatekeepers* propres aux médias traditionnels permet la publication d'une information riche et abondante. Cela opère un renversement important dans la mécanique de la visibilité et de l'attention (Cardon, 2019 ; Vaidhyanathan, 2018 ; Wu, 2017). Au sein des médias de masse, les choix éditoriaux des *gatekeepers* signifient que l'information visible mérite l'attention. Or, sur internet, ce qui est visible n'est pas nécessairement important. À examiner de plus près la manière dont ce champ informationnel est structuré, Cardon (2019) explique qu'en réalité seul un petit nombre de contenus fait l'objet d'une attention de la part des internautes.

Cette concentration croissante de l'information en ligne est l'effet de la loi de la puissance « où un tout petit nombre de sites reçoit l'essentiel des liens et où un très grand nombre en reçoit très peu » (Flichy, 2008a : 170). Cette loi de la puissance est en partie fixée par un mécanisme propre à internet, celui des liens hypertextes. Dans son sens technique, ces liens sont « a technological capability that enables one specific website (or webpage) to link with another » (Park, 2003 : 49). Pour plusieurs auteurs, il est toutefois primordial de dépasser leur simple dimension technique. Bien plus qu'un simple lien, ils sont munis d'une signification sociologique et politique basée sur un principe d'association, servant entre autres à structurer la visibilité des pages web (Hsu et Park, 2011 ; Rogers et Ben-David, 2009). Les moteurs de recherche ont un rôle clé dans ces nouveaux systèmes de hiérarchisation dans lesquels certains contenus seront rendus accessibles ou non[26] (Cardon, 2019). De manière synthétique, on peut dire que le système fonctionne comme suit :

> En comptant les liens hypertextes qu'ont reçus les sites web : un site très cité sera bien classé, un site peu cité sera enfoui dans les profondeurs des résultats du moteur de recherche. En faisant un lien hypertexte, en likant, en retweetant, en commentant un contenu, les internautes émettent un signal qui sera calculé par cet agrégateur de l'intelligence collective des internautes qu'est le moteur de recherche chargé d'effectuer un classement (p.150).

En même temps que ce mécanisme permet un accès au web plus convivial et interactif, il est également pernicieux en attirant la majorité des utilisateurs à se rassembler autour d'un faible nombre de plateformes numériques. Depuis quelques années maintenant, cette concentration

[26] À ce titre, il existe un ensemble de techniques pour optimaliser la visibilité d'une page web dans les résultats d'un moteur de recherche, connu sous le nom de *Search Engine Optimization* (SEO).

de liens hypertextes gravite autour de quelques sites dominants tels que Google, Facebook ou encore YouTube (Loader et Mercea, 2011). Pour le dire autrement, un petit nombre d'entreprises propriétaires centralisent aujourd'hui la majeure partie des contenus visibles sur le web (Couldry, 2015 ; Turow, 2012 ; Wu, 2017). À l'évidence, cette nouvelle concentration du pouvoir favorise l'accès à certains types d'informations et limite le potentiel de concurrence entre les discours politiques. Pour Loader et Mercea (2011), ces effets de domination nuancent inéluctablement le potentiel démocratique des réseaux sociaux et des moteurs de recherche.

Toutefois, même si au sein d'internet une hiérarchisation de l'information opère, il n'y aucune raison de supposer que cette concentration soit similaire à celle retrouvée dans les médias de masse (Castells, 2009 ; Benkler, 2009 ; Flichy, 2008a). Internet reste un espace ouvert où les individus peuvent plus facilement exprimer leur opinion, en évitant les biais des mécanismes marchands des médias de masse. Internet a notamment renforcé la visibilité de groupes alternatifs, marginalisés ou opprimés qui sont peu ou pas représentés dans des discours publics dominants (Dahlberg, 2007). S'il est possible de parler d'un espace plus ouvert, il n'en reste pas moins que ces groupes gravitent autour de quelques sites seulement (Flichy, 2008a).

2.1.4. De la fracture numérique à la fracture démocratique

Plusieurs recherches montrent les limites du discours utopique sur les principes émancipateurs d'internet en rappelant qu'ils existent des inégalités entre les différents groupes et individus qui utilisent ce médium (Murdock et Golding, 2004 ; Hoar et Hope, 2002 ; Schradie, 2019 ; Selwyn, 2004). Ce phénomène renvoie à ce qu'il est devenu commun d'appeler « fracture numérique » (*digital divide*). Cette notion est « utilisée pour décrire du point de vue des utilisateurs ordinaires ou du public, les inégalités d'accès aux réseaux, les inégalités d'équipements, de pratiques ou de savoir-faire » (Boullier, 2016 : 123).

Avant d'être un concept sociologique, l'auteur rappelle que la fracture numérique a d'abord été un discours politique, lancé par Al Gore en 1995. Ce slogan politiquement marqué était à cette époque binaire, puisqu'il renvoyait aux inégalités d'accès à internet : être connecté ou non (Selwyn, 2004 ; Thomas, 1996 ; van Dijk, 2006). Pour réduire la fracture numérique, la solution promue par les décideurs politiques s'est rapidement tournée vers un déterminisme technologique, où il suffirait d'améliorer la répartition spatiale des équipements de base

(comme les serveurs, les câbles, etc.) pour augmenter le taux de connexion d'une région ou d'un pays (van Dijk, 2006 ; van Deursen et van Dijk, 2019). Quoique l'écart concernant l'accès physique à internet se soit réduit dans différentes régions du monde et au sein même des pays les plus développés (van Deursen et van Dijk, 2011, 2014, 2019), plusieurs études (van Deursen et van Dijk, 2019 ; Gonzales, 2016) ont montré que les résidents à faibles revenus de pays industrialisés maintiennent des difficultés à maintenir un accès physique à internet (notamment marquée par des interruptions fréquentes de connexion).

Dans le courant des années 2000, une nouvelle vague de travaux a permis de constater qu'il existe une autre fracture numérique qui concerne cette fois-ci les compétences et le type d'utilisation qui peut être fait d'internet (Hargittai, 2002 ; van Deursen et van Dijk, 2011, 2014, 2019 ; van Dijk et Hacker, 2003). À ce titre, Selwyn (2004) note qu'il est essentiel de différencier l'accès à internet et leur utilisation. Avoir accès à internet ne signifie pas pour autant qu'il y aura une utilisation ou un engagement avec la technologie (Loader et Mercea, 2011). De plus, ce n'est pas tout le monde qui participe nécessairement au débat politique. La littérature indique que les utilisateurs les plus actifs dans les débats en ligne sont en grande partie des activistes de mouvements sociaux, politiciens et membres de partis politiques ainsi que des individus déjà pleinement investis dans des causes politiques (Loader et Mercea, 2011).

Dans le cas de la participation au débat public et de l'engagement politique en ligne, plusieurs études (Norris, 2001 ; Schradie, 2019) ont montré que l'utilisation d'internet est corrélée aux classes sociales, aux organisations et aux idéologies qui les traversent. La sociologue Schradie (2019) indique par exemple que les classes sociales les plus défavorisées ont tendance à avoir plus de difficultés à développer leur militantisme en ligne, notamment en raison d'un manque de ressources matérielles, mais également par un manque de compétences et de savoir-faire. La chercheure explique que face à une individualisation de la parole, plusieurs militants ont évoqué avoir des craintes et réticences à prendre part aux discussions. L'auteure a pu constater qu'au sein des groupes de classes moyennes et supérieures, les militants affichent plus de compétences, de ressources et de confiance pour prendre part au débat.

Cette « fracture démocratique » (Norris, 2001) signale qu'il ne suffit pas d'accéder aux conditions matérielles pour faire d'internet un lieu d'information politique et de débat démocratique. Au contraire, la participation en ligne dépend de plusieurs éléments sociaux,

psychologiques, économiques et surtout pragmatiques (Selwyn, 2004). Ainsi, « engagement with ICT is therefore less concerned with issues of access and ownership but more about how people develop relationships with ICTs and how they are capable of making use of the social resources which make access useable » (Selwyn, 2004: 349). Étant donnée la répartition inégale de la participation au débat politique, internet montre ses limites lorsqu'il est question de mettre au point des procédures réellement émancipatrices et démocratiques.

2.2. Architecture technique et formats de la visibilité

Afin de caractériser plus en détail les formats de visibilités proposés par les plateformes numériques, un point d'entrée incontournable est celui du *design de la visibilité* élaboré par Cardon (2009). L'auteur nous explique pour commencer que la manière dont les individus apparaissent sur les réseaux sociaux et dont ils interagissent avec les autres usagers est architecturée très différemment selon la plateforme numérique utilisée. Certains sites requièrent par exemple de remplir une fiche signalétique qui demande l'identité civile et sociale sans suggérer d'inscrire avec soi un réseau d'amis ou de proches. D'autres proposent au contraire à l'internaute d'utiliser un pseudo et d'inviter son réseau relationnel à se joindre à ses activités sur la plateforme. Dès lors, il existe une série de systèmes d'enregistrement, de descriptions signalétiques et d'assignations différentes qui divergent selon le type d'interface. Dans ce contexte, les médias sociaux permettent à l'utilisateur de manipuler les possibilités de visibilités offertes par les plateformes, sans pour autant rendre nécessairement tout public (Cardon, 2011 ; Kwok Choon et Proulx, 2011).

Les caractéristiques de l'architecture technique d'un site représentent donc une étape primordiale dans le processus de mise en visibilité (Proulx, 2011). Comme Lessig (2000) le mentionne : l'architecture technique définit la façon dont nous vivons dans l'espace numérique. La substance des contraintes est établie par les concepteurs du code et varie d'une plateforme à une autre ; certains espaces requièrent un mot de passe ou seront cryptés, alors que pour d'autres il ne sera pas nécessaire de s'identifier, etc. Pour l'auteur, « the code or software or architecture or protocols set these features, which are selected by code writers » (Lessig, 2000 : 125).

Ainsi, les choix du *design* de l'interface des réseaux sociaux ne sont jamais neutres. Le fait que certains comportements soient rendus possibles ou non sur les plateformes numériques

découle de choix techniques qui sont avant tout de nature éthique et politique (Benhamou, 2002 ; Lessig, 2006 ; Proulx, 2011). Effectivement, les choix technologiques sont le résultat de luttes de pouvoir et d'intérêts concurrents qu'il s'agit de qualifier de purement politiques. Les choix techniques sont donc la résultante d'une série de considérations politiques et éthiques qui restent invisibles à la plupart des utilisateurs (Proulx, 2011). Ainsi, pour l'auteur, « lorsque l'utilisateur se décrit, il a l'impression de jouir d'une complète liberté, mais, dans les faits, son expression créatrice obéit à des normes invisibles. Ces normes sont ancrées dans le dispositif, et coïncident avec les contraintes de l'architecture technique » (p.18).

Au-delà de l'architecture qui détermine la manière de se rendre visible, dans le monde numérique, les utilisateurs ont aussi les ressources nécessaires pour contrôler leur visibilité (Cardon, 2009). En effet, ils peuvent choisir ce qu'ils veulent montrer d'eux et qui peut y avoir accès. Dans ces conditions, la visibilité peut se révéler moins immédiate que dans les médias traditionnels, qui en publiant créent un espace de visibilité ouvert, global et uniforme. Les usagers des plateformes numériques sont libres de former un périmètre à leur visibilité à l'aide de jeux de masques, de filtres ou de sélection de facettes.

Les utilisateurs ont également la possibilité d'employer des stratégies d'anonymisation afin d'établir une distance entre leur personne réelle et leur identité numérique, jusqu'à ôter toute référence sur qui ils sont et ce qu'ils font dans la vie réelle. La sphère d'apparence sur internet est donc malléable et permet aux usagers de construire leur apparence numérique différemment selon la plateforme utilisée. Que l'usager choisisse de *flouter* en partie son identité ou qu'il soit dans une zone d'*hyper-visibilité*, montre que chaque plateforme suggère une politique de visibilité qui lui est propre et propose aux internautes de jouer leur identité selon des registres divers. Comme le résume l'auteur, il existe donc un véritable lien de dépendance entre l'image de soi et la structuration de l'interface.

Pour Livingstone (2008), l'architecture du site est un des facteurs essentiels du cadrage. Elle rend compte des interfaces des sites sous le vocable d'*affordance* (Gibson, 1977 ; Norman, 1999). Ce terme, issu de la psychologie cognitive, renvoie aux possibilités d'actions sur un objet et se définit comme la « capacité d'un objet à suggérer sa propre utilisation » (Proulx, 2011 : 19). En reprenant la théorisation de Hutchby sur la réciprocité entre la technologie et les pratiques sociales, Livingstone (2008) indique :

> Affordances are functional and relational aspects which frame, while not determining, the possibilities for agentic action in relation to an object. In this way, technologies can be understood as artefacts which may be both shaped by and shaping of the practices humans use in interaction with, around and through them (p.5).

Dès lors, en matière d'*affordance*, les réseaux sociaux numériques instaurent un cadrage, mais ne déterminent pas les représentations.

2.3. Les couches techniques de la visibilité

La partie précédente nous permet de comprendre la manière dont les architectures numériques induisent des formats de visibilité différents selon les sites web. Il nous reste toutefois à explorer les différentes couches techniques, qui jouent un rôle primordial dans la structuration de la participation en ligne. Considérer la dimension technique des technologies numériques permet de rendre compte des ambitions politiques des dispositifs et la manière dont ils orientent les comportements des individus (Badouard, 2014 ; Mabi, 2016). Notons d'ores et déjà qu'il ne s'agit pas ici d'y voir une approche déterministe, puisque nous continuons à considérer que l'utilisateur peut être créatif, s'approprier voire détourner l'infrastructure technique (van Dijck, 2013). Dans cette section, nous nous intéresserons au code informatique, aux algorithmes, aux données et aux protocoles.

2.2.1. Le code

Le code constitue l'une des charpentes essentielles au fonctionnement de logiciels. Dans son sens le plus restreint et le plus technique, il se caractérise par des « instructions and rules that, when combined, produce programs capable of complex digital functions that operate on computer hardware » (Dodge et Kitchin, 2005 : 163). Le code est ainsi quelque chose d'exécutable dans un environnement informatique (Berry, 2016). Plus précisément, le code se subdivise généralement en deux formes, celui du code source[27] (la forme textuelle du code écrit par les programmeurs) et celui du code exécutable (le code compilé lisible par l'ordinateur) (Berry, 2016). Se basant sur cette division Kitchin (2017) indique que le code est

[27] Le fait que la notion de code source en tant que source soit apparue provient d'un ensemble de tendances humaines à octroyer une source souveraine à une action (Chun, 2011b). Or, pour l'auteure le code source ne devient source que dans l'après-coup : « source code becomes the source of an action only after it expands to include software libraries, after it merges with code burned into silicon chips, and after all these signals are carefully monitored, timed and rectified » (Chun, 2011b :104).

toujours à situer dans une chaîne de traduction à plusieurs niveaux. L'un des premiers aspects sera de traduire une tâche ou un problème dans une formule mathématique (parfois référé comme pseudo-code). Ensuite, pour que le code exécute la tâche ou résolve le problème, il faudra traduire l'ensemble de ces instructions en code lisible par l'ordinateur. En pouvant s'implanter d'un programme à l'autre grâce à l'interopérabilité existante avec d'autres langages de programmation, le code est modulaire[28] (Schäfer, 2011).

Le code s'inscrit toujours dans une grande variété de langages de programmation et de pratiques associées :

> When we want to look at the code, we see a number of different perspectives and scales depending on what kind of code we are viewing (assembler, C++, Pascal), on its state (source, compiled, disassembled), location (embedded, system, application) or its form (textual, visual, mapped as a graph). Further, code may also be distinguished between dominant/hegemonic code and subaltern or critical code (Berry, 2016 :33).

Dans la littérature, il est courant d'associer le code à une forme de langage (Cramer, 2008). Le code est néanmoins un langage spécifique car « code is the only language that is executable » (Galloway, 2004 : 165). Il est « the first language that actually does what is says – it is a machine for converting meaning into action » (Galloway, 2004: 165-166). Ce discours est toutefois nuancé par Chun (2011a) qui estime que « code does not always or automatically do what it says, but it does so in a crafty, speculative manner in which meaning and action are both created » (p.24).

Pour MacKenzie (2003a, 2003b, 2006) le code ne peut se réduire à un mécanisme pour une machine. Comme toute technologie, le code se caractérise par un ensemble de pratiques, d'interactions, d'instabilités, de disputes et d'événements. Le code est rarement immobile, mais s'inscrit dans des interactions complexes à la fois avec d'autres processus en cours d'exécution ainsi qu'avec des utilisateurs qui à travers leur interaction avec le code produisent un résultat (Berry, 2016). L'auteur soutient que le processus d'exécution du code peut s'associer à d'autres contextes et avoir une nouvelle signification politique et esthétique ou alors rester au simple statut binaire des chiffres 0 et 1.

[28] Par exemple, le langage de programmation Python contient de nombreux modules qui autorisent de relier le code Python à d'autres langages de programmation.

2.2.2. Les algorithmes

D'un point de vue purement technique et informatique, les algorithmes sont des constructions mathématiques qui agissent sur un corpus de données, configuré pour résoudre un problème défini et accomplir certaines tâches (Gillespie, 2014, 2016 ; Miyazaki, 2012). Cette description abstraire, formalisée par une procédure de calcul (Dourish, 2016), se matérialise au sein d'une composante logique (les connaissances pour résoudre le problème) et d'une composante contrôle (stratégie de résolution de problème), donnant l'équation suivante : « Algorithme = Logic + Control » (Kowalski, 1979). À cet égard, il est devenu commun de comparer les algorithmes à une recette, qui consistent à suivre une série d'instructions étape par étape afin d'atteindre un résultat.

Actuellement, la puissance des plateformes de médias sociaux demeure dans leur capacité à inclure des opérations d'algorithmes de traitement de données, menant à un paysage médiatique de plus en plus algorithmique (Anderson, 2011 ; Bucher, 2018 ; Burrell, 2016 ; van Dijck, 2013)[29]. Ainsi, les utilisateurs ne font pas que consulter des pages web ou interagir avec d'autres utilisateurs (van Dijck, 2013). Ils sont aussi en interaction avec des algorithmes qui recommandent, trient, filtrent, résument, cartographient et répertorient les informations et le contenu du web selon des paramètres prédéfinis (Bucher, 2012, 2018 ; Kitchin, 2017 ; van Dijck, 2013). En particulier, les algorithmes déterminent ce qui gagne à être visible au sein des plateformes numériques et deviennent par là des intensificateurs de visibilité (Bucher, 2012 ; Cotter, 2019 ; Gillespie, 2014). Introna (2007) conclut par exemple que « search engines, through their undisclosed algorithms, constitute the conditions that make some websites/pages attractive or visible and others not » (p.9). Les mêmes conclusions ont été partagées par Pasquinelli (2009), pour qui l'algorithme de moteur de recherche de Google PageRank est devenu la source de visibilité la plus influente sur le web.

Les algorithmes sont en quelque sorte devenus les nouveaux gardiens de l'information (Cardon, 2015), qui se substituent aux humains habituellement responsables des choix éditoriaux et du filtrage de l'information (Barnet 2009 ; Mittelstadt et al., 2016). En

[29] En inventoriant rapidement, Gillespie (2014) observe que les algorithmes orientent le choix des informations jugées pertinentes pour nous ; que les moteurs de recherches nous permettent de naviguer dans des bases de données volumineuses contenant de l'information dispersée sur le web ; que les algorithmes de recommandation s'attèlent quant à eux à cartographier nos préférences par rapport aux autres ; que les algorithmes gèrent nos interactions sur les sites des médias sociaux ; ou encore que des algorithmes calculent les « tendances » ou les contenus « les plus discutés » pour les présenter aux internautes.

établissant les conditions à partir desquelles une information sera visible plutôt qu'une autre, ils formatent le monde d'une certaine manière. Fondée sur l'affirmation selon laquelle les artefacts techniques sont dotés de qualités politiques (Winner, 1980), la littérature récente confère davantage un pouvoir politique aux algorithmes (voir Ananny, 2016 ; Beer, 2009, 2017 ; Bucher, 2018 ; Gillespie, 2014 ; Kitchin, 2017 ; Kushner, 2013 ; Lash, 2007). Comme le stipule Bucher (2018), attribuer aux algorithmes de recommandation une dimension politique « refers to the idea that realities are never given but brought into being and actualized in and through algorithmic systems » (p.3).

L'auteur ajoute que cela oblige à être attentif au fait que si certaines réalités sont renforcées d'autres seront délaissées. En tant que tels, les algorithmes qui agissent pour filtrer et trier les contenus sur le web deviennent de puissants appareils discriminatoires en participant à configurer ce qui devrait et ne devrait pas être vu (Bucher, 2012 ; Noble, 2018). Dans ce contexte, pour Bucher (2018) il est primordial de reconnaître aux non-humains, c'est-à-dire les algorithmes, leur rôle essentiel dans la co-constitution des représentations et des façons d'être dans le monde.

La menace de l'invisibilité

Selon l'étude de Bucher (2012), les algorithmes de réseaux sociaux tels que l'algorithme de classement des flux d'actualités de Facebook EdgeRank, place les usagers non pas dans une surveillance constante, plus que dans celle d'une *menace d'invisibilité*. Partant du cadre foucaldien du panoptique, l'auteur affirme que la visibilité sur les réseaux sociaux est source de gratification et d'aspiration, plutôt que celle d'une punition et d'assujettissement. Comme l'explique l'auteur, « the problem as it appears is not the possibility of constantly being observed, but the possibility of constantly disappearing, of not being considered important enough » (2012 : 1171). Ainsi, devenir visible découlera d'un processus de sélection de multiples algorithmes (Bucher, 2012 : 1174). Dans ce contexte, l'auteur opère un renversement dans la notion de surveillance théorisée par Foucault qui consiste à faire de la visibilité permanente la principale source de menace.

Parer la menace d'invisibilité nécessite de suivre une certaine logique obtempérée par les algorithmes. Si la plupart des utilisateurs n'ont pas nécessairement connaissance de la manière dont ces algorithmes fonctionnent, lorsque ces derniers en ont conscience, ils

tenteront d'intervenir sur eux. S'inspirant de Michel de Certeau et de sa théorie sur les stratégies et tactiques de résistances quotidiennes, plusieurs études (Mannell, 2017 ; van der Nagel, 2018 ; Willson, 2017) ont montré la manière dont certains utilisateurs mettent en place des techniques de résistance pour agir sur les algorithmes. Cela permet de nuancer les multiples études qui accordent un pouvoir absolu aux algorithmes, tout en minimisant la puissance d'agir des usagers des plateformes numériques.

2.2.3. Les données

Les données des utilisateurs collectées obéissent à une double logique : la monétisation et l'entraînement des algorithmes d'apprentissage automatique. La première logique repose sur une monétisation des traces numériques laissées sur la plateforme par les utilisateurs. Comme nous l'avons brièvement vu dans le chapitre 1, la plupart des plateformes numériques basent leur modèle d'affaires sur une logique d'accumulation des données de leurs utilisateurs (Langley et Leyhson, 2017 ; Pasquale, 2016 ; Srnicek, 2017 ; Zuboff, 2015 ; 2019). Zuboff (2019) explique que la valeur économique de nombreuses plateformes dépend de la collecte des données et de leur revente à des acteurs tiers et publicitaires, qui peuvent être utilisées à des fins totalement différentes du contexte dans lequel elles sont recueillies. Les plateformes sont alors architecturées de manière à extraire à large échelle les données de leurs utilisateurs et deviennent des sortes de « surveillance systems by design » (Gates, 2019 : 63)[30].

Ces données, qui peuvent être utilisées à des fins de surveillance ou de marketing, englobent à la fois des données personnelles, démographiques ou de profilages, mais aussi des métadonnées comportementales fournies manuellement par l'utilisateur (par exemple les *tags* que les YouTubeurs attribuent à leurs entrées vidéo) ou encore de données dérivées automatiquement des *cookies*, des téléphones intelligents, des GPS, etc. (Mayer-Schönberger et Cukier, 2013 ; van Dijck, 2013). Face à cette accumulation intentionnelle et grandissante de données personnelles par les acteurs des grandes plateformes numériques, certains auteurs parleront d'une *dataification* de la société (Mayer-Schönberger et Cukier, 2013) ou encore d'un « capitalisme de surveillance » (Zuboff, 2015).

[30] Notons néanmoins que certains règlements et lois sont apparus ces dernières années pour renforcer la protection des données personnelles sur internet. C'est notamment le cas du règlement européen sur la protection des données (RGPD, 2016) ou encore du California Consumer Privacy Act (CCPA, 2018).

La deuxième logique de collecte des données personnelles se base sur la volonté de les inclure dans des modèles algorithmiques (Neyland, 2015). Si l'algorithme découle de tout un arsenal d'éléments pour fonctionner, ses opérations dépendront en partie de structures de données (Bucher, 2018 ; Gillespie, 2014 ; Fuller et Goffey, 2012). Les algorithmes contemporains, et essentiellement ceux basés sur l'apprentissage automatique, doivent par exemple reposer un corpus de données existants[31] (Gillespie, 2016). Plus précisément, afin que les algorithmes exploitent automatiquement les données, elles devront être formalisées en fonction (Gillespie, 2014). Ce faisant, « les décisions critiques ne sont pas prises sur la base de données en tant que telle, mais sur la base de données analysées par l'algorithme » (Pasquale, 2015 : 21).

Ces données sont régulièrement associées à l'idée qu'elles seraient totalement objectives, neutres et autonomes (boyd et Crawford, 2012 ; Gitelman, 2013 ; Gitelman et Jackson, 2013 ; Rouvroy et Berns, 2013). Cette conception a toutefois été vivement critiquée par la recherche. Gitelman et Jackson (2013) soulignent que parler de données, c'est dire qu'elles sont collectées, entrées, compilées, mémorisées , traitées et interprétées. Pour que les données existent et fonctionnent comme telles, elles devront d'abord être imaginées en tant que données et ensuite générées (Gitelman et Jackson, 2013 ; Manovich, 2010). Ces données sont toujours certifiées nettoyées, triées, hiérarchisées par des ensembles d'acteurs qui ont un intérêt particulier à créer de nouveaux types de données (Gillespie, 2014, 2016).

En d'autres termes, les données ont besoin des acteurs humains et ne sont pas dénuées de frictions au moment de leur constitution et catégorisation (Gitelman et Jackson, 2013). Une autre critique régulièrement soulevée explique que les données utilisées peuvent facilement reproduire des biais et des discriminations (Eubanks, 2018 ; Noble, 2018, O'Neil, 2016 ; Pasquale, 2015). Malgré qu'il puisse exister des précautions importantes pour éviter de reproduire de tels biais, « algorithmic systems may unintentionally perpetuate and reinforce historical biases because the feedback loop that these systems rely upon draws on historic data patterns that may replicate themselves in algorithmic system outputs » (Yeung, 2018 :12).

[31] L'auteur indique que pour que l'algorithme soit un minimum fiable ou utile, il faudra un ensemble massif de données sur lequel il pourra s'entraîner. Par exemple, les algorithmes de réseaux sociaux reposent sur énormément de nœuds avant d'être en mesure de décrire ou d'influencer une communauté en ligne. Une longue période d'observation des flux de données sera aussi nécessaire pour les algorithmes de recommandation et de prédiction avant qu'ils puissent effectuer des prévisions utiles.

Enfin, la prise de décision algorithmique et l'exploration de données reposent essentiellement sur des connaissances inductives et des corrélations subséquentes à des jeux de données à grande échelle. Le problème se pose dès lors de savoir dans quelle mesure ces masses de données utilisées par un algorithme produisent une « équité » dans l'action et ses effets (Mittelstadt et al., 2016). Les corrélations peuvent effectivement engendrer d'innombrables corrélations « parasites » ou incertaines dans le cas de l'analyse prédictive (boyd et Crawford, 2012 ; Mittelstadt et al., 2016). Le problème majeur est que les connaissances découlant des masses de données pourraient ne concerner que des populations, or les décisions prises par un algorithme d'apprentissage automatique sont pourtant dirigées envers des individus (Illari et Russo, 2014). Comme le résume Rouvroy (2011) :

> Fragmented as they will be into a myriad of "correlatable" data and aggregated with others with whom they do not share anything more than the simple fact of having exhibited similarly correlated biographical, behavioural, or other elements, the profiled individual[32] will not necessarily be able to contest or resist the autonomic assignation of profiles and the practical consequences ensuing in terms of access to places, opportunities, and benefits.

2.2.4. Les protocoles

Au-delà du déploiement d'algorithmes, l'architecture codée d'une plateforme se réfère à des protocoles (van Dijck, 2013). Un protocole informatique est « a set of recommendations and rules that outline specific technical standards »[33] (Galloway, 2004 : 6). Dans le cas du web 2.0, les conditions d'opérationnalisation de la circulation des contenus et de la participation des utilisateurs résultent toujours de protocoles (Langlois et al., 2009a). Des plateformes comme Facebook par exemple, mettent à disposition un ensemble d'instructions et de fonctionnalités auxquelles les utilisateurs doivent se souscrire s'ils souhaitent participer aux interactions médiatisées (van Dijck, 2013). Ainsi, pour l'auteure, « Facebook's protocols guide users through its preferred pathways; they impose a hegemonic logic onto a mediated social practice » (p.31).

[32] Certains droits ont toutefois évolué sur ce plan. Par exemple, le RGPD offre la possibilité aux individus de contester une décision lorsqu'elle se fonde sur un traitement automatisé : « The data subject shall have the right no to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her ». Voir : https://gdpr-info.eu/art-22-gdpr/

[33] Les protocoles qui encadrent une grande partie d'internet peuvent être trouvés dans ce qui est appelé les documents RFC (Request For comments). Considérés comme la « documentation principale d'internet », la majorité des normes et des protocoles utilisés par internet y sont détaillés.

Les études sur les protocoles permettent de s'affranchir des premiers appels utopiques d'un internet libertaire. Les protocoles sont un agencement technique qui doit permettre d'imposer une conduite quelconque à une multiplicité d'utilisateurs dans un milieu matériel hétérogène. Elle agit sur le réseau par son organisation interne qui opère comme un « massive control apparatus that guides distributed networks, creates cultural objects, and engenders life forms » (Galloway, 2004 : 6). Le fait qu'internet soit rarement considéré comme hautement gouverné repose entre autres sur la confusion entretenue par deux niveaux de protocole : les protocoles TCP/IP (les principaux protocoles de transmission) qui distribuent horizontalement des paquets de données d'un ordinateur à un autre ; le protocole DNS[34] (Domain Name System) qui distribue verticalement les noms de domaines d'internet à partir d'organismes de régulation. Présents depuis les débuts, les protocoles automatisent le contrôle à partir de dynamiques techniques et politiques, qui servent des intérêts spécifiques. Les protocoles sont généralement négociés par des organismes et des organisations professionnelles (par exemple l'Internet Engineering Task Force (IETF), le World Wide Web Consortium (W3C), l'Internet Corporation for Assigned Names and Numbers (ICANN)), puis matérialisés dans le monde réel par de larges populations d'utilisateurs. Malgré cette logique de contrôle, chaque utilisation continue de disposer d'une marge de manœuvre (van Dijck, 2013). Les utilisateurs, rappelle l'auteure, n'ont jamais cessé de résister ou de détourner les applications, en bricolant le logiciel de la plateforme ou en créant des applications subversives.

2.4. De nouveaux modérateurs

Après avoir indiqué les différentes caractéristiques techniques des technologies numériques et la manière dont elles implantent un certain nombre de valeurs, il faut rappeler qu'elles ne sont qu'un des aspects du processus d'organisation et de contrôle de l'environnement numérique. Ils existent au sein du web un ensemble de règles et de droits qui commandent la participation et les échanges en ligne. Cette capacité du réseau à réguler les flux informationnels et comportements illicites renvoie généralement aux modalités de modération. Malgré l'imaginaire fortement ancré qu'internet serait exempts de *gatekeepers*, « plateformes do, and must, moderate the content and activity of users, using some logistics of detection, review,

[34] Durant les années 1990 les DNS sont devenus un enjeu de conflits commerciaux et de propriété intellectuelle. Dès ce moment, l'administration Clinton a souhaité privatiser la gestion des noms de domaine et de transférer les responsabilités à un organisme créé ad hoc, à savoir l'Internet Corporation for Assigned Names and Numbers (ICANN) (Delmas, 2002 ; Massit-Folléa, 2012).

and enforcement » (Gillespie, 2018: 21). Sans la modération, les plateformes ne pourraient fonctionner (Gillespie, 2018). Il s'agit ainsi d'un mécanisme de gouvernance qui structure la participation et protège la communauté des abus (Grimmelman, 2015: 6). Dans ce qui suit, nous verrons comment les processus de régulation des contenus et comportements illicites sont distribués au sein de différents acteurs : la communauté en ligne, les entreprises privées, les pouvoirs publics. Nous commencerons toutefois par brièvement introduire la régulation sur internet, afin de pouvoir mettre en perspective les acteurs impliqués dans la modération.

2.3.1. La régulation sur internet

Une des particularités d'internet par rapport à d'autres technologies de communication est qu'il a été expérimenté et auto-administré pendant près de 20 ans par des pairs et experts informatiques, pour la plupart américains (Massit-Folléa, 2014). Lorsqu'il en était encore à ses débuts, on a souvent attribué la capacité d'internet à ébranler les formes traditionnelles de gouvernance et la réglementation étatique – qui y semblent moins praticables (Johnson et Post, 1996 ; Reidenberg, 1996 ; Trudel, 2000, 2006 ; Ziewitz et Brown, 2013). Internet était perçu comme un lieu défiant les institutions politiques traditionnelles, donnant ainsi l'illusion d'être totalement anarchique et ingouvernable ou d'être en quelque sorte « l'hydre moderne » capable de détourner toute forme de réglementation (Klein, 2002 ; Ziewitz et Brown, 2013). Cela part du principe qu'il n'existe pas de « droit de l'internet », comme il existe un droit de l'espace ou de la haute mer (Massit-Folléa, 2012). Cette vision d'un internet qui serait anarchique et incontrôlable est aujourd'hui désuète. Tout comme d'autres technologies antérieures, le cours de l'histoire montre que plus internet s'est propagé dans la société, plus il a été question de l'insérer dans les structures réglementaires existantes (Klein, 2002).

De façon générale, les études ont régulièrement montré que la régulation sur internet doit s'envisager de manière plurielle (Massit-Folléa, 2014 ; Marzouki et Méadel, 2004). La régulation encadrant les technologies numériques est pensée et produite dans des lieux étatiques, non étatiques, nationaux ou internationaux, voire dans les objets techniques (Trudel, 2006). Ainsi, « ces nœuds expriment des normativités qui sont relayées par des relais tels que les systèmes de responsabilité, les pratiques contractuelles, les processus de régulation qui assurent l'application et l'effectivité des valeurs, normes et principes contenus dans les normativités diverses prétendant encadrer les technologies » (Trudel, 2006 : 2). Comme l'explique Trudel (2000, 2006), dans la réflexion consacrée à la production des règles sur

internet, avec des nuances qui leur sont spécifiques, Greenleaf (1998), Reidenberg (1996) et Lessig (2006) estiment que la normativité sur internet s'établit à partir de quatre types de contraintes ou de processus de régulation : l'architecture technique, le marché, la loi étatique et les normes autorégulatrices. Cela revient à étudier les dynamiques de régulation des flux informationnels sur internet à partir de l'architecture, du marché, du pouvoir étatique et de la société civile dans ses capacités autorégulatrices.

2.3.2. La modération par les communautés

De par son histoire et ses caractéristiques, internet a la particularité d'accorder une plus grande part de responsabilité à l'usager dans le déroulement des interactions et la souveraineté du réseau (Trudel, 2000)[35]. Marzouki et Méadel (2004) mentionnent que l'auto-régulation promue par les pionniers a toutefois pris une autre tournure lors du développement accéléré du réseau dans les années 1990 et de l'expansion du réseau d'internautes. À ce titre, Rheingold (2000) mentionne que les communautés en ligne ont généré leurs propres modes de vivre ensemble sur internet, avec des règles, des normes comportementales, des codes, des directives de participation et d'autres formes d'auto-gouvernance et de contrôle. Plusieurs études se sont ainsi attachées à décrire ces formes d'auto-régulation par les communautés en ligne.

Baym (2000) montre par exemple qu'en l'absence de mécanismes manifestes de contrôle social, les communautés en ligne ont instauré une série de normes à partir d'une identification collective de la transgression et sur la manière de la réprimander. Dans cette perspective, la communauté en ligne correspondrait à une « entité normative autonome ». Dutton et Peltu (2007) décrivent quant à eux que certaines questions de gouvernance, comme le spam ou la fraude, sont moins du ressort de l'auto-régulation communautaire. Les collectifs en ligne sont plus actifs dans le contrôle de comportements jugés inappropriés en traitant directement avec les utilisateurs qui visent à nuire aux normes de la communauté et qui mènerait à terme à des situations d'anarchie et de chaos (Barzilai-Nahon et Neumann, 2005). Ces utilisateurs

[35] À l'origine, les échanges entre les premiers acteurs d'internet étaient régis par ce qui est appelé « la nétiquette » (Massit-Folléa, 2012). Il s'agit d'un ensemble de règles de conduite qui ont ensuite été fixées pour la première fois dans la RCF 1855 en 1995. Cette charte, consacrée aux échanges communicationnels sur internet, stipule l'importance de la courtoisie et du respect de l'autre. Pensée au sein du groupe de travail *Responsible Use of the Network* (RUN) et de l'*Internet Engeenering Task Force* (IETF) et conçue précisément pour les nouveaux utilisateurs peu familiers à la culture d'internet, le document est présenté comme « un ensemble minimum de règles d'étiquette en matière de réseau (la Nétiquette) que les institutions peuvent utiliser et adapter pour leur propre usage. (…) Il convient aussi comme ensemble minimum de lignes de conduite pour les personnes, tant les utilisateurs que les gestionnaires » (cité dans George, 2002 : 4).

prenaient habituellement le rôle de « super-utilisateur », leur donnant la légitimité d'un point de vue social et technologique de faire appliquer les règles (Roberts, 2019). Diverses formes de modération de contenu exercées par des utilisateurs volontaires ont ainsi émergé dès les premières communautés en ligne (Galloway, 2006).

Généralement, les communautés exercent différents mécanismes pour maintenir l'ordre dans le cyberespace. Les réponses peuvent être à la fois techniques (par exemple filtrer les contenus inappropriés, exclure la personne qui pose problème) et sociales (comme élaborer des codes de conduite, utiliser le blâme, faire appel aux autorités hors-ligne) (Dutton et Peltu, 2007 ; Grimmelmann, 2015 ; Matias, 2019). Cet établissement d'ajustements, de compromis, d'arrangements ne permet toutefois pas une maîtrise totale des différents conflits propres aux formations sociales en ligne, comme en témoigne la présence de *trolls* ou encore les cas de cyberhaine, cyberharcèlement ou de *revenge porn* (Citron, 2014).

2.3.3. La modération par le marché

Historiquement, la modération des contenus et comportements est un exercice attesté depuis les premières communautés en ligne. En revanche, cette régulation ne s'opère plus dans les mêmes conditions que lorsqu'internet en était à ses débuts. Dans le premier chapitre, nous avons fait ressortir qu'internet est plus que jamais devenu un agglomérat d'entreprises privées, si bien qu'elles dominent actuellement le contrôle des flux informationnels (Citron, 2018 ; Gillespie, 2018 ; Roberts, 2019). Ainsi, ce qui est nouveau pour Roberts (2019) est sans conteste l'ampleur industrielle de ces activités. À plus forte raison, pour le compte de grandes entités commerciales (réseaux sociaux, organes de presses, etc.), des professionnels sont maintenant rémunérés pour leurs services dans le contrôle et l'évaluation des contenus. Roberts (2019) capture ce phénomène sous le concept de « commercial content moderation » qu'elle définit comme :

> The organized practice of screening user-generated content posted to internet sites, social media, and other online outlets. The activity of reviewing user-generated content may take place before the material is submitted for inclusion or distribution on a site, or it may take place after material has already been uploaded (p.31).

D'une façon globale, le débat public sur la modération a été clivé, entre ceux qui critiquent les plateformes pour leur inaction et leur passivité et ceux qui y voient une véritable atteinte à la

liberté d'expression (Gillespie, 2018). Il n'en demeure pas moins que cette activité renferme une série de difficultés pour les plateformes qui l'exercent. L'auteur explique que l'une des difficultés majeures pour les plateformes est de savoir quand, comment et où intervenir dans le réseau. L'auteur note aussi que la modération nécessite un grand nombre de ressources humaines et techniques tout au long du processus (traitement du signalement, prise de décision, conséquence pour l'utilisateur, examiner les appels dans certains cas). Enfin, les acteurs de la modération doivent également être en mesure d'apprécier le caractère manifestement illicite d'un contenu (Citron, 2018 ; Greenberg, 2015 ; Hecker, 2015). Dans cette tâche, les entreprises signalent leur difficulté à évaluer les discours dits extrémistes vu le manque de consensus entre les instances gouvernementales sur cette question (Citron, 2018 ; Hecker, 2015).

Et pourtant, malgré ces obstacles, modérer les contenus et les comportements nuisibles est une pratique essentielle pour la survie des plateformes de réseaux sociaux ou tous les autres sites où les utilisateurs sont mis à contribution pour produire du contenu (Gillespie, 2018 ; Roberts, 2019). Selon les auteurs, la modération est essentielle pour deux raisons. Premièrement, il s'agit de favoriser une communauté hospitalière en modérant les contenus illégaux et violents, tout en protégeant les utilisateurs ou groupes d'autres internautes offensifs. La deuxième raison s'inscrit quant à elle dans un impératif purement économique. Dans ce contexte, la régulation par le marché est liée à la valeur que chaque firme accorde à sa réputation (Rallet et Rochelandet, 2011). Les plateformes doivent effectivement pouvoir présenter leur meilleur visage aux nouveaux utilisateurs, aux annonceurs et à leurs partenaires, ainsi qu'au grand public[36] (Gillespie, 2018). De plus, elles doivent éviter de perdre des utilisateurs qui seraient victimes de harcèlement, tout comme de faire l'objet de mesures légales lorsque celle-ci n'a pas été en mesure de respecter les lois nationales en matière de contenus haineux ou autre.

2.3.4. La modération par les pouvoirs publics

De manière générale, la place de l'État dans la régulation d'internet a fait l'objet de vifs débats au sein de la communauté scientifique. Pendant longtemps, la vision cyber utopique a eu tendance à négliger le rôle de l'État. Des études ont par la suite tenté de réfuter les modèles

[36] À ce titre, Twitter a régulièrement été mis dans une mauvaise posture. Face à la prédominance des discours haineux et du harcèlement au sein de la plateforme, plusieurs acquéreurs potentiels se sont désistés par crainte que la firme ne survive pas à un tel environnement toxique (Marwick, 2017 ; Gillespie, 2018).

antérieurs qui ont marginalisé l'intervention étatique. Par exemple, pour Drezner (2004) et Goldsmith et Wu (2006), l'État n'a jamais vraiment été marginalisé, mais seulement dépassé par des théories simplistes qui ont supposé le déclin inévitable de l'État face au réseau mondialisé. Pour d'autres (Christou et Simpson, 2009), l'État absent au début, a pu conquérir le réseau en s'adaptant aux nouvelles technologies. Van Eeten et Mueller (2013) notent que certaines de ces études tendent à gonfler le rôle de l'État dans la régulation d'internet, en lui attribuant un rôle dominant et allant parfois jusqu'à nier l'existence d'une gouvernance sur internet. Ainsi, ces diverses manières de concevoir la place des États dans la régulation d'internet ont inévitablement mené à une polarisation au sein de la recherche.

Face au recul de l'intervention étatique, la régulation d'internet a souvent été présentée comme le prototype d'un nouveau genre de régulation totalement décentralisée et exempte d'intervention publique (Brousseau, 2001). Pour l'auteur, cette vision trop simpliste est à nuancer. Comme il le rappelle, il est vrai qu'à ses débuts internet s'est déployé sur la base d'une « régulation contractuelle ou communautaire dont le principal mode de mise en œuvre repose sur la concurrence, les parties déçues par des tiers pouvant facilement redéployer leurs réseaux rationnels grâce aux propriétés techniques d'internet : notamment son caractère mondial et l'ouverture de ses normes » (p.2). L'intervention étatique apparaissait comme totalement désuète. Présentement, bon nombre de gouvernements estiment qu'internet est devenu trop important pour être laissé à la seule responsabilité d'acteurs privés ou aux normes techniques (Brousseau et al., 2012). Sans pour autant surestimer le rôle de l'État dans la régulation d'internet, il n'est plus inapproprié de reconnaître aujourd'hui l'existence d'une intervention étatique.

La régulation des États se manifeste aujourd'hui dans de nombreux lieux du réseau[37] (Marzouki et Méadel, 2004) et notamment dans le filtrage et le blocage de contenus (DeNardis, 2010 ; MacKinnon, 2012). Plusieurs auteurs (Benkler, 2009 ; Marzouki et Méadel, 2004) ont observé une forte activité législative et politique dans le secteur de l'information et des communications depuis les années 1990, en ce qui a trait à la propriété intellectuelle, à la responsabilité des acteurs ou encore au filtrage, tant au niveau national que plurinational. Les

[37] Les gouvernements souverains assurent certaines fonctions de la gouvernance d'internet comme la régulation d'abus et de fraude, la mise en place de mesures antitrust et de réponses aux menaces de sécurité sur internet (DeNardis, 2010). Aussi, les États-Unis par l'intermédiaire de leur département du Commerce sont jusqu'à récemment restés le propriétaire du système d'adressage, en déléguant la gestion à divers organismes non gouvernementaux comme l'ICAN (Brousseau, 2001 ; Marzouki et Méadel, 2004 ; Mueller, 2010).

auteurs soulignent qu'internet peut également être sous l'autorité de certains pays autoritaires où il existe des limitations d'accès à l'information étrangère par l'intermédiaire de fournisseurs d'accès placés sous leur contrôle. Plusieurs exemples démontrent également comment les plateformes numériques cherchent à satisfaire les demandes gouvernementales afin de pouvoir accéder à certains marchés fructueux. Prenons le cas du lancement de l'iPhone en Chine à l'automne 2009 (MacKinnon, 2012). Apple a dû se soumettre à une série de critères pour pouvoir délivrer son produit sur le marché chinois. Entre autres, la compagnie a dû s'engager à vérifier le contenu de toutes les applications disponibles au téléchargement sur l'Apple Store, en supprimant celles où figurait du contenu sur le Dalaï-lama ou encore sur la chef dissidente ouïghoure en exil, Rebiya Kadeer.

Les plateformes n'ont toutefois pas toujours besoin de lois nationales ou d'impositions gouvernementales pour censurer du contenu. MacKinnon (2012) indique par exemple qu'en mars 2010 Apple a supprimé sans avertissement une application iPad dédiée à *Stern*, l'un des plus grands magazines allemands. Pour cause, le magazine avait publié du contenu érotique. Malgré que ce contenu soit totalement toléré en Allemagne, certaines pages du numéro du magazine comportaient du contenu qui violait les normes d'application Apple. Face à ce puritanisme américain, la suppression de l'application a mené à la censure entière du magazine. Il faut ainsi admettre que les instances gouvernementales n'ont pas toujours d'autorité immédiate dans la modération et le filtrage de contenus sur internet. Eu égard à ce qui précède, on peut donc remarquer la complexité de la régulation des flux informationnels, qui cumule un ensemble d'acteurs, d'actions, d'ajustements potentiels et de compromis multiples.

Conclusion

Plusieurs enseignements peuvent être tirés de ce deuxième chapitre. Premièrement, on assiste depuis plusieurs années à la multiplication des études sur le rôle d'internet dans la transformation de l'espace d'apparence. Pour la majorité des défenseurs d'internet, les technologies numériques sont l'incarnation d'une démocratie en réseau centrée sur le citoyen-utilisateur ou encore la représentation par excellence d'un forum habermassien. Loin de réfuter intégralement les effets émancipateurs de ces technologies, plusieurs études se sont affranchies de ces rhétoriques utopistes. Elles ont montré les lacunes d'internet à mettre au point des procédés réellement démocratiques pour la participation au débat politique. Ces

critiques ont été principalement de trois ordres : la possibilité qu'internet renforce l'homogénéité des opinions, la concentration de l'information et la fracture démocratique.

Deuxièmement, si les activistes utilisent les technologies numériques pour rendre visible leur cause, la littérature en communication nous apprend que ces espaces numériques sont de plus en plus dominés par de grandes entreprises. Sur ce point, la recherche a montré que le paysage numérique actuel se veut plus privatisé, centralisé et clos. Sans pour autant fétichiser la dimension économique, cela permet de comprendre que les plateformes numériques sont architecturées de façon à produire du profit, ce qui ordonne certains types d'usages au détriment d'autres. Le contexte culturel, économique et social dans lequel ces technologies fonctionnent a peu été pris en compte par la recherche sur l'activisme en ligne, préférant s'intéresser aux possibilités de réalisation de militantisme à travers ces technologies.

Troisièmement, ce deuxième chapitre nous invite à prendre au sérieux l'ensemble des éléments humains et non-humains qui contribuent à former la visibilité en ligne. Il s'est attardé à montrer que l'exercice de la visibilité repose sur une architecture technique. Elle est en relation avec une série de non-humains (par exemple les algorithmes, le code ou encore les protocoles) qui implémente un certain nombre de valeurs et d'usages, de continuités et de discontinuités. Ce chapitre marque aussi l'importance de prendre en considération le fonctionnement de la régulation des contenus et des comportements illicites sur internet. Ainsi, il existe une série de normes visibles et invisibles qui sous-tendent la visibilité en ligne. De plus, en même temps qu'internet se veut un espace ouvert et habilitant, il peut également être hiérarchique et contraignant.

Pour l'heure, nous pouvons formuler une série de questions provisoires qui découlent des enseignements tirés de la revue de la littérature menée dans les deux premiers chapitres : Comment se construit et se maintient la visibilité au sein de technologies de plus en plus dominées par un oligopole ? Quel rôle jouent les non-humains (algorithmes, codes, protocoles, *botnet*s) dans le fonctionnement de la visibilité et de l'invisibilité ? Quels effets ont les usagers qualifiés d'extrémistes sur les plateformes numériques ? Laissons de côté pour le moment ces questions provisoires et attelons-nous à un travail de conceptualisation théorique. Pour arriver à analyser la visibilité en ligne, il nous faudra parvenir à assouplir la frontière à la fois concrète et abstraite entre les humains et les non-humains, la technique et la société, l'objet et le sujet. Cela implique donc de penser en termes d'association et

d’assemblage. Ce travail de conceptualisation théorique commence par remettre en cause ces dualismes couramment observés au sein des sciences sociales, pour ensuite tisser du complexe dans la compréhension de la visibilité contemporaine des militants.

PARTIE II :

Approches théoriques et méthodologiques

Chapitre 3 : (Re) penser la relation humain-technique au sein des plateformes numériques

L'objectif de ce chapitre est de présenter le cadre conceptuel qui guidera l'analyse de notre objet de recherche : la visibilité de groupes qualifiés d'extrémistes sur internet. Ce cadre théorique s'organise nécessairement dans l'affrontement des dualismes traditionnels en ce qui concerne les technologies numériques. Le but sera de tisser une toile conceptuelle capable de soutenir le rôle des non-humains dans l'action, ainsi que les interactions humains-machines. Pour ce faire, la théorie de l'acteur-réseau (Callon, 2006 ; Callon et Law, 1997 ; Latour, 2006a ; Law et Hassard, 1999 ; Law, 2009) constituera le cœur de notre cadre analytique. Il sera toutefois complété par le travail individuel de Suchman (2007) sur les reconfigurations humain-machine et par le travail collectif des *software studies*. Le fil conducteur de cette réflexion sera donc celui de la *co-construction* et des *reconfigurations* humain-machine dans le contexte contemporain des technologies numériques.

Après avoir présenté respectivement ces travaux, nous poursuivrons par un effort de synthèse de différentes thématiques qui seront apparues lors de notre conceptualisation théorique. Cela nous permettra de développer une approche particulière pour penser la visibilité médiatisée, à la suite de quoi nous formulerons notre problématique et nos objectifs de recherche. Ainsi, l'objectif ne sera pas d'articuler une théorie exhaustive servant à l'analyse de nos données, comme ce serait le cas dans une démarche hypothético-déductive. Étant donné que notre démarche de recherche se veut inductive, le but sera de présenter un ensemble de travaux qui alimenteront notre réflexion et nous permettront de constituer un cadre conceptuel pour la compréhension du phénomène étudié, à savoir la visibilité sur internet de l'État islamique.

3.1. La théorie de l'acteur-réseau

Une première manière rentable de parvenir à une compréhension des interactions humains-techniques consiste à utiliser les concepts développés par la théorie de l'acteur-réseau (ANT). Michel Callon, Bruno Latour et John Law sont généralement considérés comme les fondateurs de l'ANT (Callon, 2006 ; Latour, 2006a ; Law, 2009 ; Law et Hassard, 1999). Développée à partir des années 1970-1980, l'ANT puise ses sources dans les *sciences and technology studies* (STS) et dans la sociologie de Tarde pour qui le social ne peut se réduire à un domaine spécifique de la réalité, mais doit s'envisager au contraire selon un principe de connexion. Selon Tarde (1893, 1985), il n'y a aucune raison de séparer le social-humain d'autres associations (comme les organismes biologiques, les sociétés cellulaires, les sociétés atomiques, etc.). C'est donc vers cette direction que l'ANT nous amènera : une hybridation du social.

Plus spécifiquement, la théorie de l'acteur-réseau est « a disparate family of material-semiotic tools, sensibilities and methods of analysis that treat everything in the social and natural worlds as a continuously generated effect of the webs of relations within which they are located » (Law, 2009 : 2). Pour l'auteur, l'ANT est une application résolument sémiotique. L'ANT met au centre de son analyse l'hétérogénéité relationnelle des objets étudiés. Elle assume par ailleurs que les entités s'influencent réciproquement, à tel point qu'elles sont constitutives de la réalité. Ces formes conjuguées d'hétérogénéité mènent ainsi à deux niveaux d'analyse (Law, 1999). Le premier se rapporte à la *matérialité relationnelle* du réseau et la seconde à la *performativité* de ces relations. La notion d'*actant* empruntée à la sémiotique permet de travailler cette hétérogénéité des relations, en l'élargissant à toutes les entités qui interagissent dans le réseau et qui y introduisent une modification dans le déroulement de l'action (Callon, 2006 : Latour, 1994).

Cet accent mis sur la dimension relationnelle d'entités hétérogènes permet de dépasser un vocabulaire dualiste largement répandu au sein des sciences sociales et de la philosophie (ou comme le dirait Latour (1991b) chez les modernes) : technique/social, nature/société, humain/non-humain. Ce qui intéresse l'ANT est *à la fois* la technique et le social (Akrich, 1992 ; Latour, 2000). Cette façon d'entrevoir la « non-séparabilité » des objets et des sujets nourrit une critique de la « sociologie du social ». Son principal reproche est que la sociologie du social a trop rapidement clos la sphère du social (Latour, 2006a). En d'autres mots, selon

la sociologie du social, le monde social existe toujours déjà, il est une substance, un type de matériau spécifique. Or pour l'ANT, la société et le social ne sont jamais donnés de prime abord. Plutôt que d'être un domaine spécifique, le social est le mouvement particulier d'un assemblage de liens. Cette approche préconise ainsi la nécessité pour l'enquêteur d'analyser plusieurs « régimes de vérités », plusieurs types de raison, plusieurs modes d'existence. Autant de façons qui risquent de plonger le chercheur dans une incertitude sur ce que constitue une action, un groupe social, une technique, la science ou encore la politique (Latour, 2012).

Si dans ce qui suit, nous présentons les postulats centraux à l'ANT, avant de poursuivre vers sa conceptualisation des objets techniques, nous nous autoriserons à effectuer certains rapprochements avec des travaux qui présentent des propriétés très proches avec la théorie de l'acteur-réseau tels que ceux de Deleuze et Guattari, Haraway ou encore DeLanda. Selon Bingham (1996) ces travaux peuvent être rassemblés sous la même étiquette d'approches « matérielles-sémiotiques », en ce qu'ils portent leur intérêt sur la manière dont se construisent, se maintiennent et se stabilisent des relations entre des collectifs hybrides. Les éléments qui composent l'ANT sont principalement de six ordres :

> There is *semiotic relationality* (it's a network whose elements define and shape one another), *heterogeneity* (there are different kinds of actors, human and otherwise), and *materiality* (stuff is there aplenty, not just "the social"). There is an insistence on *process* and its *precariousness* (all elements need to play their part moment by moment or it all comes unstuck). There is attention to *power* as an effect (it is a function of network configuration and in particular the creation of immutable mobiles), to *space* and to *scale* (how it is that networks extend themselves and translate distant actors). (Law, 2009 :146)

3.1.1. L'hétérogénéité du social

Callon et Latour indiquent qu'aucune vie sociale ne peut être pensable « without the participation – in all the meanings of the word – of nonhumans, and especially machines and artifacts » (1992 : 359). Dans la même veine, Haraway soulignait que « the world has always been in the middle of things, in unruly and practical conversation, full of action and structured by a startling array of actants and of networking and unequal collectives » (1992 :304). Pour ces approches, la gamme d'acteurs impliquée dans l'action doit être élargie (Latour, 2006a), puisque l'ordre social émane de la coexistence d'éléments hétérogènes (Callon et Law, 1997 ; Whatmore, 2002).

Malgré qu'il s'agisse d'un principe qui semble à première vue évident (personne ne nierait que la société est peuplée d'objets), leur prise en charge théorique reste néanmoins quelque chose d'ardu, au point que la sociologie est trop souvent restée « sans objet » (Latour, 1994). De prime abord, elle a toujours accordé plus d'importance à l'étude des groupes ou des liens sociaux, l'amenant ainsi à surestimer les relations interpersonnelles dans l'interaction sociale (Conein, Dodier et Thévenot, 1993). Les objets ont quant à eux souvent été négligés, voire absents de la sociologie. Et quand ils étaient abordés, le statut des objets a longtemps alterné entre celui de fétiche, n'étant rien d'autres que l'écran de nos projections et celui de contraintes naturelles, rigides, mettant de l'avant l'objectivité des forces de la nature (Latour, 1994 ; 2000). Manifestement, la controverse sur ce qui est entendu par objet bute sur la polarité entre le mauvais et le bon objet : « ou bien ils sont totalement manipulés par les humains ; ou bien ce sont eux, au contraire, qui manipulent à leur insu, les humains » (Latour, 1994 : 559). Ce faisant, l'objet est toujours une ressource ou une contrainte, mais jamais un acteur à part entière.

À cette asymétrie, il est nécessaire de rétablir une symétrie entre celui des choses et des humains (Latour, 1991b). La place de l'objet doit être modifiée, en l'extrayant de la *chose-en-soi* pour le conduire vers le collectif. Est-ce dire que les choses et les humains sont équivalents ? Aucunement, selon Latour. À la notion de symétrie, il explique qu'« être symétrique pour l'ANT signifie simplement de ne pas imposer *a priori* une fausse asymétrie entre l'action humaine intentionnelle et un monde matériel fait de relations causales » (Latour, 2006a : 109). Face à cette redistribution de l'agir à tous les êtres, les entités en question cessent d'être des intermédiaires. Plutôt, elles deviennent des médiateurs, c'est-à-dire des « acteurs dotés de la capacité de traduire ce qu'ils transportent, de le redéfinir, de le redéployer, de le trahir aussi » (Latour, 1991b : 111)[38].

Comme le rappelle Latour (2006a), les objets ne doivent pas se comprendre comme déterminant l'action ou comme s'ils agiraient à la place des acteurs humains. Cela serait une ineptie, puisqu'il s'agirait de considérer cette fois-ci les objets comme des causes dont les

[38] Reconnaître une puissance d'agir (*agency*) à toutes entités non-humaines, rappelle les théories de l'action distribuée et située développée par Schuman (Barbier et Trépos, 2006). Par action située, Schuman indique qu'il s'agit de simples actions exercées dans un contexte de circonstances particulières et concrètes. La théorie de l'ANT conçoit justement que l'action est dépendante de « ses circonstances matérielles et sociales, et notamment des *affordances* fournies par l'environnement : dès lors que le déroulement d'un cours d'action conduit à repérer et à mobiliser tel ou tel artefact jusqu'alors demeuré à l'arrière-plan, ce sont de nouvelles perspectives d'action qui vont être suggérées et autorisées » (Barbier et Trépos, 2006 :38).

effets seraient véhiculés par une action humaine. Plutôt que de déterminer une action ou de simplement y incarner un rôle de figurant, les choses peuvent « autoriser, rendre possible, encourager, mettre à portée, permettre, suggérer, influencer, faire obstacle, interdire et ainsi de suite » (Latour, 2006a : 103-104). Voilà une dimension qui permettra de mettre en avant un aspect inédit de la visibilité sur internet : le rôle des objets techniques dans sa constitution et son fonctionnement.

3.1.2. Des connexions entre des acteurs hétérogènes

Comment penser le rôle des non-humains dans la visibilité de l'État islamique ? Décrire la visibilité sur internet nécessite de penser l'ensemble des objets techniques et des humains participants à l'action non pas comme des entités séparées, mais comme des entités assemblées. Lorsque Callon décrit la domestication des coquilles Saint-Jacques dans la baie de Saint-Brieuc (Callon, 1986), les électrodes des piles à combustible (Callon, 1989), la mise sur le marché du véhicule électrique en France (Callon, 1979), quand Latour décrit la bactérie de l'anthrax atténuée par Pasteur (1984) ou encore la clé de Berlin (1993) et quand Law décrit l'avion de combat de la British Royal Air Force (RAF) (Law et Callon, 1992), on voit émerger une multiplicité d'éléments associés qui résultent d'un « processus de composition » (Callon et Law, 1997 : 104). La tâche de ces différentes réflexions vise à démontrer que la société, la science ou les objets techniques ne peuvent être pensés que de manière relationnelle (Law, 2009).

Ces différents travaux présentent des propriétés très proches avec le concept d'agencement de Deleuze et Guattari (1980). Deleuze entend par agencement : « une multiplication qui se compose de nombreux termes hétérogènes et qui établit des liaisons, des relations entre eux » (Deleuze et Parnet, 2007 :69). L'assemblage devient un co-fonctionnement, une symbiose. Ce qui importe, ce sont les alliances et les alliages. Si les liens entre ces deux théories ne sont que peu cités, pour Law (2009) l'ANT serait en quelque sorte une version empirique de la philosophie de Deleuze et Guattari [39]. Au cœur de ces théories se trouve l'idée que le déroulement d'une action s'effectue rarement d'humain-à-humain ou d'objet-à-objet. Plutôt, l'action noue, croise et fusionne des entités humaines et non-humaines (Latour, 1991a, 1991b ; 2006).

[39] Dans le texte de Latour (1999) visant à redéfinir l'ANT, ce dernier a suggéré que l'ANT aurait pu s'appeler « actants-rhizome » en référence à Deleuze et Guattari.

Cette association entre différentes entités conduit les tenants de l'ANT à parler « d'extériorité des relations ». Pour parler de cet *extérieur* des relations, Latour évoque la figure du « plasma ». Il appelle plasma : « cet espace – mais ce n'est pas un espace – dans lequel reposent – mais il n'y a pas de repos – les circulations diverses de totalisations et de participations en attente d'explication et de composition » (Latour, 2007 : 6). Ainsi, le plasma permet de faire référence à un « ensemble de phénomènes non formatés » (Latour, 2006a : 351). Il s'agit d'un arrière-plan en attente de socialisation ou d'engagement dans des chaînes métrologiques[40]. Cet en-dehors est « overwhelming, excessive, energetic, a set of undecided potentialities, and an ultimately undecidable flux » (Law, 2004 : 144).

En faisant référence à cet arrière-plan, « non formaté » à partir duquel émergent les assemblages, Latour créé un nouvel agent extérieur à la médiation des entités. Ce nouvel agent sera suivi d'un nouveau programme d'action qui articulera une nouvelle proposition, un nouvel objectif (Latour, 2001). La spécificité de ce nouvel objectif est qu'il n'est déterminé par les programmes d'actions d'aucune des entités engagées. Cette attention portée à l'extériorité des relations a également été pensée par les théories de l'assemblage avec notamment DeLanda (2006). Ce dernier met l'accent sur le fait que les entités en relation ne sont pas entièrement déterminées par cette relation. L'association d'entités hétérogènes fera toujours l'objet d'un excédent, de quelque chose qui se trouve en dehors des relations et qui permet de se brancher à d'autres agencements. Ainsi, la médiation qui s'opère entre des acteurs humains et non-humains doit se comprendre sous la doctrine de l'émergence de la nouveauté.

L'acteur-réseau

Eu égard à ce qui précède, nous avons maintenant les ressources théoriques nécessaires pour répondre à la question qu'est-ce qu'un acteur-réseau ? Un acteur dans la perspective de l'ANT est toute entité « qui définit et construit (avec plus ou moins de succès) un monde peuplé d'autres entités, les dote d'une histoire, d'une identité et qualifie les relations qui les unissent » (Callon, 1991 : 205). Pour le dire plus simplement : l'acteur est le résultat d'une association d'éléments hétérogènes. Il devient ce point trouble qui « constitue autant de points d'arrêt, d'asymétries ou de pliures » (Deleuze, 1989, cité dans Callon, 1991 : 209). De prime

[40] La méréologie est un terme savant utilisé par Latour pour désigner « le rapport des parties au tout » (Latour, 2007 : 123).

abord, le fait d'associer un acteur à un réseau et d'intégrer à cette catégorie les non-humains, le distingue des acteurs traditionnels de la sociologie (Callon, 1987).

Au sein de l'ANT, l'acteur advient à la suite d'un réseau qui est structuré de relations hétérogènes. Quant au réseau, il demeure relié à la description. Il n'est pas une *chose-en-soi*, plus qu'un concept qui aide à décrire tout regroupement (Latour, 2006a). L'acteur et le réseau sont comme les deux faces d'une même abstraction : un réseau d'acteurs ne peut aucunement se réduire à un seul acteur, tout comme il ne peut se réduire à un seul réseau (Callon, 1987). Si l'acteur est un effet de réseau, il devient légitime de se demander en quoi un acteur se différencie d'un intermédiaire. A priori, un acteur ne diffère nullement d'un intermédiaire (Callon, 1991). Le qualificatif d'acteur adviendra lorsqu'il fera l'objet d'un mécanisme d'attribution. Ainsi, un acteur est « un intermédiaire auquel la mise en circulation d'autres intermédiaires est imputée » (Callon, 1991 : 206).

Callon (1991) explique que ce réseau d'acteurs n'est toutefois jamais prévisible. Le fait que les entités qui le composent peuvent être humaines ou non-humaines, à tout moment elles peuvent « redéfinir leur identité et leurs relations mutuelles d'une manière nouvelle et apporter de nouveaux éléments au réseau » (Callon, 1991 : 1987). Les éléments du réseau se caractérisent ainsi par une instabilité. Leur identité quant à elle se définira toujours au fil des associations.

La traduction

Avant de passer à notre dernière section sur la manière dont l'action est traitée au sein de l'ANT, un dernier éclaircissement doit être effectué. Tentons maintenant de répondre à la question : comment ces entités hétérogènes seront-elles mises en relation dans la perspective de l'ANT ? Ces imbroglios socio-techniques ne seront autres que le résultat de traductions (Callon, 1986 ; Callon et Law, 1997). La traduction vient opérer la jonction entre les acteurs ou les intermédiaires, qu'ils soient collectifs ou individuels, humains ou non-humains. Loin de se satisfaire de cette unique fonction, la traduction est sous-tendue par un potentiel de transformation des éléments en relations et de la composition de nouveaux buts (Callon, 1991 ; Latour, 2006a, 2001).

Dans son texte sur la domestication des coquilles Saint-Jacques et des marins-pêcheurs dans la baie de Saint-Brieuc, Callon (1986) montre que traduire dépend de toute une série d'opérations. Cela implique à la fois des opérations de cadrage, de mobilisation et de coordination. Parmi celles-ci, il faudra formuler une problématisation (devenir un « point de passage obligé »), mobiliser des porte-parole qui parleront au nom de tous, attribuer et définir des rôles (enrôler) et sceller des alliances (intéresser). L'ensemble de ces « formes de coordination » (Callon, 1991) cherchent à produire le même résultat, celui de ratifier l'ensemble des acteurs au sein de traductions stabilisées.

La traduction n'est jamais donnée en soi, mais agit de manière évolutive (Callon, 1991). L'auteur décrit plusieurs cas de figure. La traduction peut parfois être trahison, source de désaccord ou objet de contestation. À l'autre extrémité, l'alignement des différentes entités peut se faire sans entraves. Dans ce cas de figure, la traduction se révèle dans la plénitude d'une communication parfaite, d'une entente entre les entités et d'une absence d'ambiguïté. Entre les deux, explique l'auteur, il y a ces situations où la traduction se stabilise à la suite d'une série de négociations et d'itérations plus ou moins longues et difficiles. Ainsi, « la traduction réussie créé cet espace commun, cette équivalence, cette commensurabilité qui manquaient : elle *aligne*, tandis que si elle échoue, A et B retournent à leur incommunicabilité, se reconstruisant, en se *désalignant*, des espaces sans commune mesure » (Callon, 1991 : 212).

3.1.3. Des collectifs actifs

Il est maintenant légitime de se demander : Qui exécute l'action ? Pour l'ANT, c'est l'agent n° 1, l'agent n° 2, l'agent n° 3… (Latour, 2001). En somme, l'action tient tout entière dans l'association d'humains et de non-humains (Latour, 1994 ; 2001 ; Callon et Law, 1997) et nécessite de traiter l'action comme un problème sémiotique (Haraway, 1991). L'action est ainsi l'« effet généré par un réseau de matériaux hétérogènes en interaction » (Law, 1992 : 383). En cela, elle s'articule toujours au sein d'une médiation. Prenons l'exemple donné par Callon et Law (1997) d'Andrew, directeur d'un gros laboratoire :

> Il serait erroné d'affirmer que Andrew est un stratège. C'est le collectif hybride : (Andrew + fax + secrétaire + organisme de direction + ministère + trains + PC + chercheurs + notes d'information + système d'enregistrement des budgets-temps +….), qui doit être considéré comme une capacité stratégique. (p.112).

L'action dans la perspective de l'ANT s'inscrit dans un double mouvement de prolongement et de débordement (Callon et Law, 1997). Elle relaie une série d'activités qui ont commencé avant elle. Elle est répétition, contenue dans un prolongement. Dans la mesure où l'action est une médiation à travers laquelle se déplacent des formes d'existences diverses, elle est toujours débordée ou dépassée (Latour, 1994, 2006). Les entités, qu'elles soient humaines ou non, débordent l'action en ce qu'elles la relancent et y participent en ses propres termes.

Comme le stipule Latour (1994), un acteur n'agit jamais seul : on le fait agir. Chaque entité ne peut passer à l'action qu'à travers un réseau d'association qui le dépasse (Latour, 1994). Par conséquent, l'action n'est jamais localisable, elle est toujours *dislocale* et quant à son origine, elle est toujours incertaine (Latour, 2006a). Cette conception de l'action ouvre ainsi un nouveau dialogue sur son attribut. Plutôt que d'établir sa source, comme c'est traditionnellement le cas, l'ANT propose « l'abandon de la question de la source de l'action au profit de sa redistribution ou de sa dissémination » (Callon et Law, 1997:100). L'attribut de la source devient ainsi celui du collectif hybride. On peut certes attribuer à un des acteurs le rôle premier de moteur, cela n'enlève pas que seule « la composition de l'action peut rendre compte de l'action » (Latour, 2001 : 192). Cette redistribution complète de l'action rappelle qu'elle n'est « jamais une affaire cohérente, contrôlée, rondement menée, dont les contours seraient bien définis » (Latour, 2006a : 67).

Lorsqu'on affirme qu'un acteur –individuel ou collectif- ne constitue pas le point de départ d'une action, le réflexe est alors généralement de penser qu'il est réduit à des forces extérieures. Or, « faire, c'est faire faire. Quand on agit, d'autres passent à l'action » (Latour, 1994 : 601). Ainsi, l'acteur ne peut se réduire à un champ de force – une structure : l'action ne peut être que distribuée avec d'autres actants. Penser en termes de médiation, permet d'extraire l'action d'une dichotomie entre d'un côté des acteurs et de l'autre des champs de force : « il n'y a que des acteurs – des actants – dont chacun ne peut passer à l'action qu'en s'associant à d'autre qui vont le surprendre, le dépasser » (Latour, 1994 : 601). Ceci impose une position antiréductionniste vis-à-vis du social, ou un principe d'irréduction (Latour, 1984). Ce principe adopte l'idée selon laquelle « aucune chose n'est de soi-même réductible ou irréductible à aucune autre – jamais de soi-même, mais toujours par une autre » (p.244).

La mise en boîte noire de l'action

Une des spécificités de la théorie de l'acteur-réseau est que l'action conserve toujours une part de mystère. Pour les tenants de l'ANT, chaque action collective est mise dans une boîte noire (Callon, 1987, 2006 ; Latour, 2001 ; Law, 1987, 2009). Cette opération de « mise en boîte noire » de l'action collective rend « totalement opaque la production conjointe d'acteurs et d'artefacts » (Latour, 2001 : 192). Cela répond à un principe de simplification, nécessaire à l'organisation d'associations hétérogènes et à la durabilité du réseau (Callon, 1986, 1987 ; Law, 1987). Les entités hétérogènes qui participent à l'action le font ainsi souvent de manière silencieuse et invisible (Callon, 2006). Dans l'exemple que donne Callon (2006) sur l'automobile, lorsqu'un conducteur tourne la clé du volant de sa voiture, c'est tout un réseau d'action collective parfaitement coordonnée qui se déclenche (des compagnies de pétrole qui ont raffiné et distribué le pétrole aux feux rouges qui régulent le flux de la circulation). Cette action collective sera mise dans une boîte noire, sous la forme cette fois-ci d'un artefact ; l'automobile.

Cette mise en boîte noire de l'action collective reste néanmoins toujours provisoire (Callon, 2006 ; Callon et Law, 1997). L'action se révélera par des controverses, des échecs ou des incidents (Callon, 2006). Les entités sont ainsi toujours provisoirement stabilisées, à tout moment elles peuvent reprendre leur indépendance et céder à un essaim de nouveaux acteurs (Callon, 1991 ; Callon et Law, 1977). Aussi étrange que cela puisse nous sembler, si une entité paraît en apparence être délimitée par des « frontières » ou une « enveloppe », en pratique elle est « simultanément distribuée dans tous les éléments dont elle est composée » (Callon et Law, 1977 : 109). C'est donc bien là notre intérêt, ouvrir la « boîte noire » de la médiation technique qui sous-tend la visibilité sur internet de groupes définis comme extrémistes et de saisir les liens complexes et provisoires entre les plateformes et les militants.

3.1.4. L'objet technique dans la perspective de l'ANT

Occupant une place centrale dans notre thèse, intéressons-nous maintenant à l'objet technique en tant que tel. Tout au long de notre thèse, nous parlerons en effet de plateformes, de *botnets*, de logiciels, de matières informatiques, d'algorithmes, etc. Or comment conceptualiser tous ces objets qui peuplent la visibilité de l'État islamique ? L'ANT a particulièrement porté son attention sur la construction des faits scientifiques et des objets techniques. Son approche de la technique comme réseau s'apparente au modèle de « tissu sans couture » développé par

Thomas P. Hughes (1983). Cette notion a été proposée par ce dernier pour « rendre compte de l'hétérogénéité des éléments associés dans ce que Hughes appelle un système technologique et de l'impossibilité qu'il y a à découper dans ce système des pièces d'une texture uniforme, que celle-ci soit sociale, technique, ou économique » (Akrich, 1994 : 16).

Figurer la complexité des techniques

Traditionnellement, la technologie, et plus largement la technique, est envisagée sous deux angles : celui du déterminisme technique et celui constructivisme sociologique. Le premier se fonde sur l'hypothèse que les techniques seraient gouvernées par des forces internes et s'autogénéreraient (voir par exemple Gille, 1978 ; Ellul, 1977). En leur attribuant une logique autonome, on voit se déployer l'idée d'un progrès unilinéaire et d'une force exogène s'acharnant à exister hors de la société. Au sein de ces théories, les techniques sont munies d'un pouvoir, celui d'avoir des effets profonds et immédiats sur la société, sans que le monde social puisse l'influencer en retour.

Cette perspective a été remise en cause par le constructivisme social des technologies (Bijker, Hughues et Pinch, 1987 ; Pinch et Bijker, 1987). Ces théories montrent que le développement des techniques n'est pas linéaire, mais se divise en un ensemble de ramifications. Distinction faite, les auteurs plaident qu'il existe une « flexibilité interprétative » (Bijker et al., 1987 : 40). Effectivement, pour ceux-ci, les objets techniques ne sont pas dépourvus de flexibilité en ce qui concerne la manière dont les usagers pensent et interprètent les objets techniques. Le constructivisme social pose également une opposition ferme en ce qui a trait à la question de l'autonomie des techniques, puisqu'il s'agit cette fois-ci de raconter les techniques selon un processus culturel et social.

Si ces théories ont le mérite d'envisager la codétermination entre les entités techniques et humaines, le risque est de ramener la conception du dispositif à des déterminations qui seraient uniquement sociales (Akrich, 1989, 1994). Par ces nouvelles déterminations, l'objet technique resterait neutre jusqu'à son insertion dans des circonstances sociales et politiques (Grint et Woolgar, 1995). Selon les auteurs, bien que ces théories soient anti-essentialistes, elles prescrivent néanmoins à l'idée que la technique puisse avoir un effet. Non pas par les caractéristiques inhérentes à la technique cette fois-ci, mais via l'incarnation des intérêts politiques et sociaux en son sein. Or, comment envisager les relations qu'entretient le

dispositif technique avec son environnement, en le réduisant « au rang d'une production presque organique, émanant d'un individu ou d'un groupe socialement marqué » (Akrich, 1989 : 32) ?

Tomber dans le « piège » de ce que le Law (1994) appelle le « réductionnisme machine », en essentialisant la technique ou encore de celui du « réductionnisme sociologique », en réduisant la technique à un processus uniquement social, revient finalement à la même conséquence, c'est-à-dire celle de négliger « those crowds of non-humans mingled with humans » (Bingham, 1996 : 636). Il faut dès lors dépasser la distinction nette effectuée entre « l'infrastructure matérielle » et la « structure sociale », pour en montrer leur *complexité* (Latour, 1991a ; Mol et Law, 2002). Disons pour faire bref à ce stade, que la technologie doit être envisagée à partir de réseaux complexes qui englobent à la fois des facteurs sociaux, politiques, économiques et techniques, qu'ils soient humains ou non-humains (Mol et Law, 2002). Cette découverte de la « multiplicité » renforce l'idée que nous ne vivons plus dans un monde qui serait à situer dans une seule *épistémè*. Ainsi, le recours à la complexité est une façon de pointer la diversité des ordres – modes d'ordonnancement, logiques, styles, répertoires, discours – qui les constituent (Mol et Law, 2002). Pour les auteurs, « la multiplicité concerne donc les coexistences à un moment donné » (p.8).

L'hétérogénéité de l'objet technique

Tout comme le social découle de chaînes d'association entre des acteurs hétérogènes (Callon, 1986, 2006 ; Callon et Law, 1997 ; Latour, 1991a, 2006 ; Law, 2009), la technologie incarne également des chaînes d'association entre des humains et des non-humains (chercheurs, technologues, ingénieurs, usagers, industriels) (Akrich, 1992 ; 2010 ; Callon, 1987, 1991 ; Callon et Latour, 1981 ; Hugues, 1983 ; Kline et Rosenberg, 1986 ; Latour, 1989, Von Hippel, 1988). Cette association d'éléments hétérogènes vient cimenter l'expression devenue courante de « tissu sans couture » proposée par Hughes (1987) ou encore d'« interdépendances techniques » (David, 1986). Ces types de considérations résistent à la notion de frontière et rendent compte de la manière dont la technique est « society shaped » et « society shaping » (Hughes, 1987 : 51). Ces chaînes d'associations qui composent les objets techniques ont amené les tenants de l'ANT à parler de « réseau-socio-technique » (Latour et al., 1991), d'« agencement socio-technique » (Callon et Muniesa, 20013) ou encore de « dispositif socio-technique » (Muniesa et al., 2007). C'est ici qu'en raison de la multiplicité des mondes

différents qui se chevauchent et coexistent au sein d'internet, nous nous autorisons à parler d'internet en tant que dispositif socio-technique[41]. Cet aspect sera toutefois mis plus avant dans la perspective des *software studies*, troisième volet de notre cadre théorique.

Pour étudier les conditions et les mécanismes en vertu desquels ces relations s'établissent et transforment à la fois notre connaissance et nos sociétés, il faudra effectuer des déplacements entre l'intérieur et l'extérieur de l'objet technique (Akrich, 1992). Ces déplacements que l'enquêteur doit accomplir soulèvent deux questions essentielles. La première est de préciser de quelle façon et dans quelle mesure ce qui compose un objet technique contraint les « actants in the way they relate both to the object and to one another » (Akrich, 1992 : 206). La seconde question se rapporte aux attributs des actants et de leurs liens, et plus particulièrement à la manière dont ces assemblages façonnent l'objet technique et aux différentes façons de l'utiliser. La frontière entre l'intérieur et l'extérieur d'un objet est donc précisément l'effet de cette interaction plutôt qu'un élément déterminant. Elle devient cette ligne de démarcation qui se déploie dans une « géographie de la délégation » entre les actions assurées par l'objet technique et les compétences d'autres acteurs (Akrich, 1992).

Cette conception déconcerte les idées sur la politique et le pouvoir qui ne sont plus seulement des intentions humaines, mais qui se réalisent également à travers des médiations techniques qui cherchent à imposer des obligations (Feenberg, 2004). Latour (2001) a par exemple montré comment les gendarmes couchés ont réussi à matérialiser dans une autre mode d'expression des normes qui obligent l'automobiliste à ralentir. Le gendarme couché est ainsi la concrétisation d'une obligation morale. Cette *délégation* des fonctions aux humains et aux non-humains peut également se comprendre comme un *shifting-out* ou un changement de scène, en ce sens qu'elles sont déplacées d'une matière à une autre (Feenberg, 2004).

Akrich (2010) apporte néanmoins une nuance en stipulant qu'il est inexact de penser que le pouvoir et la politique s'incarnent uniquement dans le simple fait de transférer des normes dans un autre mode d'expression.

> Les objets techniques ont un contenu politique au sens où ils constituent des éléments actifs d'organisation des relations des hommes entre eux et avec leur environnement. Les objets techniques définissent dans leur configuration une certaine partition du

[41] Par soucis de concision nous utiliserons le vocable de « dispositif technique » dans la suite de la thèse, n'enlevant en rien la dimension sociale de l'objet technique en question.

> monde physique et social, attribuent des rôles à certains types d'acteurs – humains et non-humains – en excluent d'autres, autorisent certains modes de relations entre ces différents acteurs, etc. de telle sorte qu'ils participent pleinement de la construction d'une culture, au sens anthropologique du terme, en même temps qu'ils deviennent des médiateurs obligés dans toutes les relations que nous entretenons avec le « réel ». (p.205).

L'objet technique comme programme d'action

Les caractéristiques de l'objet technique sont définies par des concepteurs qui imaginent un certain nombre d'hypothèses sur les éléments qui incarnent le monde dans lequel « l'objet est destiné à s'insérer » (Akrich, 2010 : 208). Cela fait dire aux tenants de l'ANT que les objets techniques disposent d'un script, d'un scénario, d'un programme d'action destiné à des mises en scène, que les utilisateurs sont amenés à imaginer en partant des prescriptions et du dispositif technique. Le dispositif technique en tant que programme d'action coordonne ainsi un « ensemble de rôles complémentaires, tenus par des non-humains (qui constituent le dispositif) et par des humains (diffuseurs, utilisateurs, réparateurs…) ou d'autres non-humains (accessoires, systèmes intégrés) qui en forment les périphériques ou les extensions » (Callon, 1991 : 2000).

Ainsi tout comme un auteur et un lecteur se saisissent à partir d'une page imprimée, le constructeur et l'utilisateur des machines se rencontrent dans leurs applications (Feenberg, 2014 ; Woolgar, 1991). C'est précisément en cela que les machines sont comparables aux textes « parce qu'elles aussi inscrivent une "histoire", c'est-à-dire une séquence d'opérations prescrites que l'utilisateur initie et subit » (Feenberg, 2014 : 91). En considérant que l'objet technique est porteur d'un « script » ou d'un « programme d'action », le rôle des utilisateurs est ici crucial (Akrich, 1992). Tant qu'aucun acteur n'interprète les rôles créés par le concepteur (ou n'en inventera de nouveaux) l'objet technique restera une illusion. Il n'y a que par la confrontation que l'objet technique se réalisera ou s'irréalisera.

En entrevoyant l'objet technique comme l'intégration de programmes d'action, nous nous rapprochons du concept de stratégies élaboré par Michel de Certeau (Feenberg, 2004). Les objets techniques ne sont pas des *choses-en-soi*, mais des « nœuds dans un réseau qui inclut aussi bien des humains que des dispositifs jouant des rôles enchevêtrés » (Feenberg, 2004 : 91). L'ANT préconise que les alliances sociales au travers desquelles la technique est conçue soient liées à ces mêmes artefacts en train d'être produits. Ce sont par ces jeux d'alliances que

les groupes sociaux émergent en même temps que la technique. Ils ne précèdent pas les objets techniques, ils apparaissent à la suite d'une confrontation avec l'objet technique. Il s'agit là d'un autre aspect de la symétrie de l'humain et du non-humain, qui distingue l'ANT des formulations habituelles des théories constructivistes.

Prenons un temps d'arrêt et voyons comment les enseignements de cette section s'articulent à notre objet d'étude. L'ANT propose un programme de recherche qui se détourne de la question de savoir ce que les dispositifs techniques font aux gens. Elle tente au contraire de saisir les agencements entre les usagers et le dispositif technique. Ce faisant, plutôt que d'étudier ce qu'internet produit sur les militants de l'État islamique, nous étudirons plus largement comment les militants de l'État islamique, par leurs usages, façonnent aussi ce que la technologie peut faire. C'est en insistant sur ces agencements que nous privilégions une approche symétrique entre les usagers et les concepteurs des dispositifs techniques. En cela, nous verrons avec notre cas comment la visibilité émerge à travers et par ces jeux complexes d'alliances, mais aussi de trahisons.

3.2. L'interaction humain-machine selon Suchman

L'anthropologue Lucy Suchman est notamment connue pour avoir développé une théorie de l'action située proche du courant ethnométhodologique, en envisageant le cours de l'action comme étant intimement liée aux circonstances environnantes et sociales. Toutefois, notre intérêt pour les travaux de Suchman se restreint au concept de reconfiguration et d'assemblage humain-machine développé dans son dernier ouvrage *Human-Machine reconfigurations* (2007), qui consiste en une réédition du précédent.

Dans cet ouvrage, Lucy Suchman marque son éloignement des approches théoriques de l'information des interactions humain-machine en articulant son projet théorique autour du concept de reconfiguration. Le caractère de ce que Suchman décrit comme reconfiguration s'inscrit dans un sens similaire à celui de la configuration : « one form of intervention into current practices of technology development, then, is through a critical consideration of how humans and machines are currently figured in those practices and how they might be figured – and configured – differently » (Suchman, 2007 : 227).

En envisageant l'interaction humain-machine sous l'angle de reconfigurations mutuelles et

permanentes des relations entre humains et machines est une façon pour Suchman de dépasser la vision qui consiste à entrevoir l'interaction humain-machine comme une conversation entre humains et machines par le biais de l'interface. Il s'agit plutôt de penser l'interaction humain-machine comme des assemblages créatifs qui « explore and elaborate the particular dynamic capacities that digital media afford and the ways that through them humans and machines can perform interesting new effects » (Suchman, 2007 : 281). Par ce fait, l'anthropologue sous-entend le besoin de repenser les configurations de plus en plus complexes et intriquées entre l'humain et la machine.

L'ouvrage de Suchman s'inspire de plusieurs domaines d'études tels que l'étude des interfaces humain-machine, les études féministes, les études des sciences et technologies et les études sur les nouveaux médias. Les travaux de Suchman nous permettront ainsi d'élargir l'unité d'analyse des interactions humain-machine en insistant davantage sur la dynamique et les multiples formes de configurations qui participent aux assemblages machines-humains. Il sera aussi question des différences et plus spécifiquement des asymétries à l'intérieur de ces assemblages.

3.2.1. Revoir la symétrie humain-machine

Suchman reprend à l'ANT et aux études en sciences et techniques le projet de proposer pour les sciences sociales une approche qui soutient le principe de symétrie pour étudier les relations entre les humains et les machines. Toutefois, Suchman plaide pour une réélaboration du concept de symétrie. En citant les travaux de Pickering et de Collins, l'auteure pointe que si l'on peut effectivement reconnaître la constitution profondément mutuelle des humains et des objets techniques, ces configurations ne vont pas nécessairement être symétriques. L'auteure rappelle que les objets techniques et les personnes ne vont pas se constituer de la même manière au sein de ces assemblages.

Suchman souhaite ainsi réarticuler le principe d'asymétrie ou de « dissymétrie », qui reconnaît la figure d'hybride, de cyborg ou encore de quasi-objet rendue visible à travers l'étude des technologies, sans perdre en même temps les particularités distinctives au sein de ces assemblages. L'auteure pointe que le fait de reconnaître les relations entre les humains et les machines n'augure en rien que ces entités soient démunies de différences. Le problème devient finalement de comprendre « the nature of difference differently » (Suchman, 2008 : 260).

Outre cet aspect, l'auteure indique que de mettre trop d'emphase sur le principe de symétrie pourrait générer ou reproduire des inégalités. Il est certain que l'appel notamment effectué par l'ANT pour une *symétrie généralisée* dans l'analyse des sciences sociales a permis de réintroduire de la matérialité et de la technique, auparavant trop souvent exclues des considérations sociologiques. Toutefois ce principe peut-être plus problématique quand il est transporté dans d'autres milieux, comme celui de la technique et de l'ingénierie. À l'inverse, l'objet technique et la machine dominent, alors que le social et l'humain sont relayés aux marges des préoccupations. Dans ce contexte, il s'agit de redonner de la vigueur à la puissance d'agir de l'homme, tout en évitant de rétablir les dichotomies classiques entre l'humain et la technique :

> We need a story that can tie humans and non-humans together without erasing the culturally and historically constituted differences among them. Those differences include the fact that, in the case of technological assemblages, persons just are those actants who configure material-semiotic networks, however much we may be simultaneously incorporated into and through them. (Suchman, 2007 : 270).

3.2.2. La relation humain-machine

Dans la perspective de Suchman, les interactions humain-machine, lorsque définies de manière large, peuvent se comprendre comme des assemblages ou des configurations particulières. L'auteur approche la question de l'assemblage de personnes et de machines dans une perspective similaire à celle en STS. Il s'agit également pour Suchman de proposer une autre lecture de la figure de cyborg développée par Donna Haraway (1991). Une des richesses de la figure de cyborg est, comme le rappelle l'auteure, d'avoir permis de nouvelles formes d'analyse inédites de la rencontre entre humains et machines. Sa faiblesse est toutefois d'avoir pris pour appui une stratégie centrée sur une figure héroïque (qu'elle soit monstrueuse ou marginalisée) qui présume une identité stable et singulière et qui néglige des assemblages entre humains et non-humains qui seraient distribués dans des sites plus quotidiens et plus banals.

Notamment, la manière dont les assemblages humains et non-humains se forment dans les entrelacs contemporains doit être envisagée dans leur complexité. À défaut de préfigurer une relation sans entraves, il faut envisager les difficultés associées à l'assemblage d'entités machiniques et humaines. À titre d'exemple, Suchman restitue plusieurs études qui attestent

des difficultés inhérentes à l'ajustement des corps à des artefacts techniques (par exemple les prothèses qui blessent les corps en même temps qu'elles permettent de nouvelles possibilités) qui peut être moins harmonieux et plus douloureux que ne le prédit le trope du cyborg. C'est en envisageant l'ordre des contraintes et de ses différents degrés de manifestation au sein de la relation humain-machine, que l'assemblage d'entités machinique et humaine diffère sensiblement de ce que la figure de cyborg permet de mettre en lumière.

Si Suchman ne réfute pas la figure de cyborg, elle propose de la réarticuler dans le champ d'assemblages socio-techniques complexes. En d'autres termes, « now that the cyborg figure has done its work of alerting us to the political effects, shifting boundaries, and transformative possibilities in human–machine mixings, it is time to get on with investigation of particular configurations and their consequences » (Suchman, 2007 : 275–276). Ainsi, l'assemblage permet d'entrevoir le travail de configuration qui participe à la constitution d'hybride. Par ailleurs, l'emphase mise sur les difficultés d'association que peuvent rencontrer ces agencements représente un point crucial pour notre étude. Notre enquête montrera notamment la manière dont les militants de l'État islamique sont constamment exclus des plateformes numériques. Plus qu'un assemblage paisible, c'est un assemblage douloureux qui sera à l'étude.

3.2.3. Penser la question des frontières

À la question des assemblages se pose inévitablement celle des frontières. S'inspirant de l'approche du réalisme agentiel de Karen Barad, Suchman pose la frontière de l'interface humain-machine comme étant essentiellement performative. Les travaux de Karen Barad, ont posé la question de la reconfiguration d'un point de vue des études féministes et des STS. Elle a en quelque sorte proposé une forme de constructivisme-matérialiste, une façon pour l'auteure de dépasser le débat entre constructivisme et réalisme. Le réalisme agentiel de Barad repose sur une relecture des travaux de Niels Bohrs. Il s'agit d'une théorisation de l'enchevêtrement qui a pour unité ontologique de base le phénomène, plutôt que celui d'un « independent objects with independently determinate boundaries and properties » (Barad, 2007 : 33). Les phénomènes se caractérisent par « the ontological inseparability of agentially intra-acting components » (Barad, 2007 : 33).

La notion d'*intra-action* est centrale dans le travail de l'auteure. Pour Barad, le néologisme d'intra-action désigne « the mutual constitution of entangled agencies » (2007: 33). Cette

perspective permet de dépasser l'idée assez convenue selon laquelle il existe des entités distinctes qui précédent l'interaction. L'intra-action reconnaît au contraire que « agencies do not precede, but rather emerge through, their intra-action » (Barad, 2007 :33). C'est par ces actions intra-agentielles que se tracent les frontières et se définissent les propriétés des composantes des phénomènes et que des concepts particuliers deviennent significatifs. La coupure entre sujet et objet est ainsi happée par les intra-actions. Dans le réalisme agentiel de Barad, les intra-actions ne remplissent pas des fonctions, mais procèdent à créer de la possibilité et de l'impossibilité ; à promulguer ce qui compte et ce qui est à exclure ; à produire des limites et des propriétés à l'intérieur des phénomènes. Elles opèrent comme des « coupes agentielles » qui sont à la fois ontiques et sémantiques. Ces coupes agentielles contribuent à « enact[s] a resolution within the phenomenon of the inherent ontological (and semantic) indeterminacy » (Barad, 2007 :140). Avec le projet théorique de Barad, il s'agit de prendre en compte :

> aspects of each in dynamic relationality to the other, being attentive to the iterative production of boundaries, the material-discursive nature of boundary-drawing practices, the constitutive exclusions that are enacted, and questions of accountability and responsibility for the reconfigurings of which we are a part. It does not take the boundaries of any of the objects or subjects of these studies for granted but rather investigates the material-discursive boundary-making practices that produce « objects » and « subjects » and other differences out of, and in terms of, a changing relationality. (Barad, 2007 :93).

Pour Suchman (2007), le réalisme agentiel de Barad permet une compréhension très différente de l'interface humain-machine. L'accent sur les effets performatifs d'assemblages particuliers permet de rappeler que les « boundaries between human and machine are not naturally given but constructed in particular historical ways and with particular social and material consequences » (Suchman, 2007 :285). Le réalisme agentiel de Barad déplace ainsi l'idée que l'interface serait une entité établie a priori, aux contours fixes. Au contraire, elle est le fruit de coupes agentielles réalisées de manière contingente. Toute la question est alors d'examiner les pratiques socio-matérielles qui affectent à la fois les personnes et les machines en tant qu'entités distinctes et qui, en retour ordonnent des formes particulières d'opérations sujet-objet. Cela permet un nouvel abord des interfaces humain-machine en tant que moment de rencontres multiples plus ou moins alignées, se produisant au sein de configurations socio-matérielles.

3.2.4. Porter attention à la figuration

Les travaux de Suchman accordent une attention particulière à la question de la figuration en prenant pour perspective les travaux récents des études féministes et culturelles des sciences. La question de la figuration a notamment été discutée dans les travaux d'Haraway, pour qui tous les langages, incluant les plus techniques et mathématiques, sont figuratifs. En cela, ils sont constitués de tropes qui allèguent des associations entre différents niveaux de significations et de pratiques. Dans cette perspective, Suchman conçoit que les technologies sont une forme de « figurations matérialisées » (Suchman, 2007 : 227). L'auteure (2012) définit la figuration de la manière suivante :

> [It] is an action that holds the material and the semiotic together in ways that become naturalized over time, and in turn requires "unpacking" to recover its constituent elements. It is also, however, a mode of production, as the circulation of figures implies their recontextualization, multiplicity and at least potential transformation. (p.49).

C'est précisément parce qu'elle invite à penser la constitution des assemblages de choses et de sens dans des agencements plus ou moins stables, que cette notion sera précieuse. Ces arrangements seront en retour constitutifs de l'association entre humain et machine. Cela prescrit une forme d'intervention méthodologique qui veille à examiner de manière critique la façon dont l'humain et les machines sont représentés dans ces pratiques. Les effets de la figuration sont pour Suchman politiques, dès lors que « discourses, images and normativities that inform practices of figuration can work either to reinscribe existing social orderings or to challenge them » (Suchman, 2007 : 227-228). Ce point particulier des travaux de Suchman nous conduit à ajouter une unité d'analyse supplémentaire à l'étude de notre cas, en tenant compte du domaine de la pratique et de la signification. Pour reprendre les termes de Suschman, cela nous permettra de voir comment les militants et les technologies sont configurés – ou figurés ensemble – dans des discours et des pratiques, et comment ils pourraient être reconfigurés ensemble autrement.

3.3. Les softwares studies

Maintenant que nous avons établi l'hybridité du social à travers l'ANT et les formes de reconfigurations entre machine et humain avec les travaux de Suchman, il nous reste un point à éclaircir : les systèmes informatiques qui se trouvent au cœur de notre recherche. Pour cela, nous nous tournerons vers les *software studies*. C'est au cours de la dernière décennie que les

softwares studies ont émergé. Champ d'étude interdisciplinaire, Fuller (2008) stipulait à cet égard que les « software studies propose that software can be seen as an object of study and an area of practice for kinds of thinking and areas of work that have not historically « owned » software » (p.2). Ces études se sont établies entre autres en opposition à une vision réductionniste et purement machinique des logiciels (Chun, 2011b ; Fuller, 2008). Les *software studies* insistent notamment sur la nécessité d'entrevoir les logiciels comme « une fonction et un langage, mais aussi une fonction et un fonctionnement, un "dire" et un "faire" sociotechnique » (Maédel et Sire, 2017 : 11). Dans cette optique, il s'agit d'étendre la compréhension du logiciel à une dimension socio-technique et culturelle (Dodge et al., 2009). En cela, les *softwares studies* ne sont pas bien différents des approches mobilisées ci-dessus. Elles nous permettront néanmoins de jeter un regard critique sur le logiciel, en comprenant la manière dont il est produit et se déploie dans le fonctionnement du monde (Kitchin, 2014a).

3.3.1. Logiciel et software studies

Avant d'entrevoir la question des *software studies* sous l'angle des médias, il est pertinent de s'arrêter brièvement sur ce qu'est un logiciel. Or comme nous le verrons dans ce qui suit, il est extrêmement ardu de dresser les contours et les frontières de ce qui définit le logiciel, tant il fait l'objet de nombreux débats et controverses au sein du courant. Cela démontre que le logiciel ne fait pas l'objet d'un consensus, mais qu'il se rattache au contraire à une diversité de conceptions et d'approches théoriques. Malgré ces différences de définitions, le courant des *software studies* a néanmoins le mérite d'arrimer une réflexion sur le statut même de la matière numérique et de ses dispositifs computationnels (Gras, 2015). Nous verrons dans ce qui suit trois conceptions du logiciel qui ont traversé les *softwares studies*.

Une compréhension matérielle du logiciel

Il existe généralement une distinction entre le terme logiciel, compris comme étant immatériel et le matériel informatique (*hardware*) qui comprend l'ensemble des composantes physiques, c'est-à-dire les ordinateurs, les serveurs, les commutateurs réseau, les câbles, etc. Or, pour un certain nombre d'auteurs, malgré l'intangibilité apparente des logiciels, ces derniers ne peuvent se concevoir sans une compréhension matérielle (Drucker, 2013 ; Fuller, 2008 ; Hutchby, 2001 ; Jackson, 1996 ; Kallinikos et al., 2012 ; Kittler, 1995 ; Leonardi, 2007, 2010, 2012 ; Leonardi et Barley, 2008 ; Orlikowski, 2007 ; Schäfer, 2011 ; Suchman, 2000 ; van den Boomen 2009 ; Volkoff et al., 2007).

Pour les auteurs qui préconisent une approche matérielle des logiciels, il faut éviter d'envisager les logiciels web comme une « substance métaphysique » qui flotterait dans un « espace virtuel » (Schäfer, 2011). Ce détour est sans conteste non négligeable, puisque trop souvent l'association des ordinateurs, des télécommunications numériques et des technologies de l'information est présentée comme un espace virtuel immatériel où la dématérialisation et l'hyper-mobilité en sont ses caractéristiques propres (Adams, 1997 ; Drucker, 2013 ; Kirschenbaum, 2008 ; Sassen, 2002). Cet « espace autre » a renforcé l'idée d'un « univers parallèle » (Benedikt, 1991 : 15), d'un « nouveau type d'espace invisible » (Batty, 1993 : 615) où se concrétise l'opposition binaire du réel et du virtuel.

Kittler (1995) dans sa formule populaire et provocatrice *there is no software* soutient qu'établir une distinction entre logiciel et matériel est totalement vain, puisque le logiciel repose constamment sur du matériel. Cette critique s'insère plus particulièrement dans les problèmes de dissimulation liés au logiciel qui « hide the very act of writing » (p.147), c'est-à-dire le code nécessaire à son fonctionnement. Notons toutefois que ce commentaire est fait du point de vue de l'utilisation finale du logiciel, puisque du côté des programmeurs l'acte d'écriture est clair et contient un ensemble de procédures, comme nous l'avons vu dans le chapitre 2 (section 2.2.3).

La question du visible et de l'invisible au sein des logiciels

La théoricienne des médias Wendy Hui Chun (2011a) propose d'envisager les logiciels dans une dialectique du visible et de l'invisible. Elle situe ainsi les logiciels dans une « essence visiblement invisible », puisqu'ils sont ce tout invisible qui engendre « the sensuous parts » (Chun, 2011a : 10). Pour l'auteure, le logiciel est une forme d'*illumination* qui permet de comprendre la partie invisible de la matière informatique. Cependant, l'auteure souligne un paradoxe : si le logiciel est un mode de dévoilement, ce qu'il illumine c'est l'inconnu. Les logiciels dévoilent ce qui est intelligible, tout en masquant ce qui génère (comme la machine) des effets visibles (Chun, 2005). Pour Chun, il faut également ramener ontologiquement le logiciel du côté des *choses* :

> understanding software as a thing does not mean denigrating software or dismissing it as an ideological construction that covers over the "truth" of hardware. It means engaging its odd materializations and visualizations closely

> and refusing to reduce software to codes and algorithms—readily readable objects—by grappling with its simultaneous ambiguity and specificity (Chun, 2011a : 11).

Plaçant ainsi le logiciel dans une épistémologie de la perception, la proposition de Chun est finalement de réintroduire le logiciel dans des problèmes visuels et idéologiques pour le comprendre, sans passer directement au domaine purement machinique.

Galloway (2012) nuance cependant cette vision occulo-centrée. Si l'auteur ne cherche pas à nier cette intrication profonde du logiciel avec le visuel, il n'en reste pas moins que cet appel à la connaissance visuelle « must still be understood in a figurative, not literal (i.e. optical), sense » (2012 : 63). Il s'agit ainsi pour l'auteur de rompre avec une potentielle fétichisation de l'interface physique. Il rappelle à cet égard que les conditions pour qu'un logiciel apparaisse ne s'expriment pas seulement à travers la visualité de l'interface. Il est le fruit d'une série d'autres technologies que l'auteur s'attelle à lister : les interfaces non optiques (clavier, souris, capteur) ; données en mémoire et données sur disque ; algorithmes exécutables ; technologies et protocoles de réseau ; etc. Ainsi, avec Galloway le spectre des technologies sous-jacentes aux technologies s'élargit[42]. Le domaine de la vision par ordinateur et de l'infographie ne constitue qu'une infime partie de l'informatique, « which occupies most all of its time with algorithms, data structures, cryptography, robotics, bioingormatics, networking, machine learning, and other nonvisual applications of symbolic systems » (2012 :64).

Laissant la question du visuel irrésolue, Galloway (2012) renvoie les logiciels à un effet d'interface. Les interfaces ne sont pas à comprendre ici comme des objets stables, mais comme des processus. La nature des interfaces est avant tout composite, puisqu'il s'agit d'un ensemble de médiations qui produisent des effets et qui sont elles-mêmes la conséquence d'autres effets. Résistant à une tentation médiacentrique incarnée entre autres par Macluhan, pour qui l'homme serait externalisé en des médias, ou encore au déterminisme technologique de Kittler qui considère que les objets médiatiques ont leur propre logique technique et ne croisent qu'occasionnellement des perceptions humaines, Galloway (2012) préconise une vision de la *technè* comme, entre autres, des pratiques vécues. Cela réside dans la volonté d'établir un contraste entre « media (as objects or substrates) and practices of mediation (as

[42] Notons que le nouveau manuel des *software studies* édités par Fuller (2008) associe également les logiciels à tout un ensemble d'éléments techniques : algorithmes, code, codecs, fonctions d'interfaces, programmes, variables, code source, etc.

middles or interfaces) » (Galloway, 2012 :16). L'auteur propose ainsi d'entrevoir les logiciels comme un ensemble de médiations où le matériel informatique est associé à ses représentations (Gras, 2015), permettant de dépasser une chosification du logiciel.

Le logiciel, un « neighborhood of relations »

Dans son ouvrage *Cutting code : software and sociality*, Mackenzie (2006) stipule la nécessité de prendre distance de l'approche formaliste préconisée par Manovich. Pour cause, ce dernier part du principe que les nouveaux médias doivent faire appel à la science informatique pour souligner les caractéristiques des médias devenus programmables : « c'est là que nous pourrons trouver des nouveaux noms permettant de désigner les concepts, les catégories et les opérations caractéristiques des médias programmables » (Manovich, 2010 : 129). Pour Mackenzie faire usage des termes de l'informatique (comme variabilité, modularité, transcodage tels que décrits par Manovich) mènerait à plus de problèmes qu'il n'en résoudrait. S'inscrivant dans une approche à mi-chemin entre les *cultural studies* et la théorie de l'acteur-réseau, Mackenzie propose d'étudier les logiciels comme étant pris dans des relations sociales qui sont le produit d'un « *neighborhood of relations* » (2006 : 10).

Le logiciel, en tant que code informatique, se tisse au sein d'une multitude de relations qui existent selon différentes classes d'unités : initiateur, prototypes et destinataires. Ces multiples classes d'unités peuvent comprendre à la fois « people, situations, organizations, places, devices and practices » (Mackenzie, 2006 : 169). Cette attention à la multiplicité des relations est également partagée par Berry (2016) pour qui le code doit être pensé tant à travers la machine que les programmeurs et les utilisateurs. C'est en raison de cette multiplicité de relations que le logiciel sera l'effet de certaines formes performatives et d'asymétries de pouvoir.

Faire de la multiplicité des relations une propriété centrale du logiciel et du code, exige selon l'auteur de l'envisager avec ses spécificités, ses singularités et ses modes d'existence. Ces formes d'interdépendance et d'articulation entre différentes relations résorbent ainsi la vision qu'il s'agirait d'une application banale ou d'une infrastructure à situer dans des changements techniques et sociaux plus globaux (comme ceux d'une « révolution informationnelle », d'une « culture digitale » ou encore de l'avènement d'une « société en réseau »). Dans la perspective de Mackenzie, il s'agit dès lors d'analyser les logiciels comme on le ferait pour la sociabilité,

c'est-à-dire « as a material object, as a means of production, as a human-technical hybrid, as a medium of communication, as terrain of political-economic contestation » (2006 : 2).

3.3.2. Médias et software studies

L'importance d'étudier les médias sous l'angle des *softwares studies* est pour la première fois mise en évidence par Manovich (2010), lorsqu'il avance que « de l'étude des médias, nous passons à quelque chose que l'on pourrait appeler "l'étude des logiciels" (*software studies*) : de la théorie des médias, nous passons à la théorie des logiciels » (p.129). Si Manovich est l'un des premiers à avoir formalisé l'étude des médias du point de vue des *software studies*, d'autres travaux ont adressé la nécessité d'étudier la question des médias sociaux à partir des logiciels, sans nécessairement en utiliser le terme. Par exemple, Beer (2009) indique que compte tenu de l'accroissement des médias sociaux et de ses algorithmes, « there is a pressing need to explore with some details this vision of power through the algorithm operating in their incorporation into users' lives » (p.999). Niederer et van Dijck (2010) ont renouvelé l'appel d'étudier les dimensions socio-techniques des applications web 2.0 en soulignant que « non-human actors and coded protocols are often overlooked in the many optimistic Web 2.0 theories » (p.1384). Si nous nous référons à la définition de van Dijck dans son ouvrage *The culture of connectivity*, techniquement parlant, les plateformes de médias sociaux :

> are the providers of software, (sometimes) hardware, and services that help code social activities into a computational architecture ; they process (meta)data through algorithms and formatted protocols before presenting their interpreted logic in the form of user-friendly interfaces with default settings that reflect the platform owner's strategic choice (2013 :29).

Cette définition démontre que lorsque l'usager interagit en ligne, il n'est pas seulement en relation avec les autres internautes, mais avec de la matière informatique telle que du code, des algorithmes, des protocoles, des programmes informatiques ou encore des interfaces. Dans la littérature récente, plusieurs auteurs ont commencé à porter leur attention sur les dimensions socio-techniques des médias sociaux et leur influence sur les modes de participation et d'usage en ligne (Gehl, 2014 ; Gillespie, 2010 ; Langlois et al., 2009b ; Langlois et Elmer, 2013 ; Niederer et van Dijck, 2010 ; Schäfer, 2011 ; van Dijck, 2013). Ces travaux ont l'avantage d'inclure un ensemble résolument hétérogène d'entités humaines et non-humaines dans l'analyse des médias sociaux.

Les *softwares studies* appliquées aux médias sociaux permettent ainsi de travailler cette exigence méthodologique de prendre en compte le rôle des non-humains dans les formes de participation en ligne. En ces termes, les plateformes numériques sont concernées par des questions à la fois techniques, culturelles, sociales et économiques (Gillespie, 2010) qui auront une incidence sur « the meaning of participation itself, as well as the meaning of related technologies, their socio-political framing and their legal regulation » (Schäfer, 2011 : 17). Ainsi, les *software studies* invitent à penser la participation en ligne à partir d'un ensemble de pratiques hétérogènes négociées entre les composantes techniques et les différentes catégories d'utilisateurs (ingénieurs, citoyens, activistes, etc.) (Langlois et al., 2009a).

3.4. La visibilité médiatisée à la lumière d'une perspective matérielle-sémiotique

Il est maintenant temps d'articuler les trois réflexions développées ci-dessus et d'en faire un cadre unifié. C'est en attachant une grande importance à réintroduire de la complexité dans l'analyse des technologies numériques que notre cadre théorique déconstruit les dualismes traditionnels. Aussi, c'est en insistant sur la participation des non-humains dans l'action que nous rétablirons le principe de symétrie dans l'étude de la visibilité médiatisée. Il est impossible d'expliquer cette articulation entre l'humain et la technique dans les phénomènes de visibilité par des théories instrumentalistes et fonctionnalistes. Tout comme il est impossible de l'expliquer en fétichisant la dématérialisation associée aux nouvelles technologies. Il faut partir d'une analyse qui envisage la manière dont les assemblages humains et non-humains façonnent cette visibilité médiatisée. Dès lors, nous pourrons envisager le problème des technologies de communication et de l'activisme d'une tout autre manière.

Notre cadre analytique repose sur l'argumentaire suivant : (1) la visibilité médiatisée doit s'envisager comme *une relation* d'entités humaines et non-humaines (2) au sein de laquelle ces entités *se reconfigurent* mutuellement et (3) s'accompagnent d'un ensemble *de mouvements* et de mutations. Par ailleurs (4) penser la visibilité médiatisée implique de la situer dans *son contexte socio-technique.* Voyons en détail ces quatre fondements principaux dans ce qui suit.

1° La relation : Nous appréhenderons la visibilité médiatisée à partir de l'imbrication d'interactions matérielles et immatérielles et multi-agents. Le front de l'analyse se trouve considérablement déplacé d'une approche déterministe des technologies ; c'est sous l'angle de la *matérialité-relationnelle* (Law, 1994 : 4), que la visibilité médiatisée devra se comprendre. Elle consiste à reconnaître que chaque entité humaine ou non-humaine, matérielle ou immatérielle est productive au sein de ces relations. L'attribut de la visibilité médiatisée devient ainsi celui d'un collectif hybride, ce qui nous oriente à redistribuer l'action à beaucoup plus d'agents que ne le prévoit le scénario instrumentaliste ou fonctionnaliste.

Cette compréhension de la visibilité nous permet de déboucher sur une perspective relationnelle qui dépasse la simple relation entre celui qui voit et celui qui est vu, comme il est coutume de l'observer en sciences sociales (Brighenti, 2010). En restant à ce niveau de relation, elle ne rend pas compte de toutes les connexions, les structures fines, les subdivisions, les ramifications qui forment la visibilité en tant que telle. Mais il faut bien s'entendre : les acteurs humains ou non-humains qui participent à façonner la visibilité, ne sont jamais totalement déterminés ou enrôlés par ces relations (Callon, 1991). À tout moment, ils peuvent redéfinir leur identité et leurs relations mutuelles (Callon, 1991 ; Suchman, 2007). Par ailleurs, ce que nous enseigne l'ANT c'est que ces assemblages d'entités hétérogènes donnent lieu à de nouveaux programmes d'actions. Cela nous amène à notre deuxième fondement.

2° La reconfiguration : Suivant Suchman (2007), le deuxième fondement part d'un postulat qu'il faut dès à présent écarter : l'interaction entre l'humain et les technologies numériques ne serait qu'une simple conversation entre humains et machines par le truchement d'une interface. Or, l'interaction humain-machine, dans l'instance de son apparition et de son mode d'être, sous-tend un ensemble de reconfigurations mutuelles. Aucune de ces entités ne sort indemne de cette relation : la technique formate les usages tout comme les usages formatent la technique (Akrich, 2006). La visibilité médiatisée est le principe même de l'imbrication d'une agentivité humaine et d'une agentivité technique, dont les frontières ne sont pas données a priori, mais se traceront au fur et à mesure des reconfigurations. Concevoir cette agentivité conjointe, c'est essayer de rendre visible et analysable cette si proche relation qui constitue l'élément de possibilité de la visibilité. Sans perdre de vue la nature distinctive de ces entités, il faut tout autant considérer les difficultés associées à l'assemblage de ces différentes entités humaines et non-humaines. Aussitôt, il faudra prendre en compte les controverses, les

difficultés, les échecs, les transitions, les moments de stabilités autour desquels gravitent et se forment ces relations.

3° Le mouvement : Du fait que les entités humaines et non-humaines se reconfigurent mutuellement et continuellement, la visibilité médiatisée se caractérise par un ensemble de mouvements et de mutations. Une réflexion théorique qui s'accompagne d'une pensée du mouvement fait résolument écho à la philosophie deleuzienne. Monnoyer-Smith (2013) explique que lorsque Deleuze a reconceptualisé le dispositif de pouvoir foucaldien (sous le concept de *diagramme*), il s'est interrogé sur les mutations et les changements au sein des dispositifs. Dans la perspective deleuzienne, il n'y a pas de diagramme qui représenterait déjà un monde existant. Si on peut parler de diagramme, c'est dans la mesure où « il produit un nouveau type de réalité, un nouveau modèle de vérité. (…). Il fait l'histoire en défaisant les réalités et les significations précédentes, constituant autant de points d'émergence ou de créative, de conjonctions inattendues, de continuums improbables » (Deleuze, 1986 : 43). Les actants qui sous-tendent tout type de visibilité médiatisée ne répondent à aucun rapport déterminable a priori ; mais sont imprévisibles et non-linéaires. Dès lors, la visibilité médiatisée sera constituée de points de contingences, de basculements et de ramifications multiples. Nous le redirons ainsi inlassablement : on n'a pas dit grand-chose sur la visibilité médiatisée si on n'entre pas dans une pensée relationnelle et du mouvement.

4° le contexte socio-technique : Parler de visibilité médiatisée nécessite de la replacer dans son contexte socio-technique. Cela implique de commencer par l'hypothèse que les technologies numériques ne doivent pas être considérées comme de simples intermédiaires, mais comme une *médiation technique* (Latour, 2001). L'objet technique dans cette perspective se caractérise davantage par une individuation (Simondon, 1958) impliquée dans une multiplicité de relations sociales, économiques et technologiques, certaines humaines, d'autres non-humaines. Envisager la technologie en tant que relation constitutive permet d'éviter de verser dans un « sociologisme » ou dans un « technologisme » en ce qui a trait à comprendre ce que la technologie *est* et *fait* à l'humain (Akrich, 1993 ; Latour, 2001). Suivant cette perspective, étudier les technologies numériques s'oppose à les considérer comme un espace virtuel désincarné de toute matérialité et de son contexte social ; la description des technologies numériques s'adresse au contraire à l'ensemble de son « contexte socio-matériel » (Robey, Raymond et Anderson, 2012). Code, données, algorithmes, interfaces, langages, matériels périphériques, corps, sont autant d'éléments qui font exister les

technologies numériques et qui les offrent à mille usages ou transformations possibles. Ce faisant, la visibilité médiatisée s'intègre dans des technologies qui sont « embedded in both the technical features and standards of the hardware and software, and in actual societal structures and power dynamics » (Sassen, 2002 : 366).

C'est donc par le biais de ce cadre conceptuel que nous analyserons la visibilité médiatisée des groupes dits extrémistes dans le contexte contemporain des technologies numériques.

3.5. Problématique et objectifs de recherche

La problématique de cette thèse a pour noyau dur la visibilité de groupes extrémistes sur internet. L'importance reconnue du rôle des technologies de communication dans la diffusion de propagande extrémiste a ouvert la voie à de nombreux travaux qui ont mis en lumière les stratégies communicationnelles de ces groupes pour se rendre visibles et maximiser cette visibilité (Awan, 2017 ; Blaker, 2015 ; Bloom et al., 2019 ; Ceron et al., 2018 ; Farwell, 2014 ; Gates and al., 2015 ; Huey et al., 2017 ; Klausen, 2015 ; Piazza et Guler, 2019 ; Richards, 2016 ; Winter, 2015 ; Zelin, 2015). L'avènement du web 2.0 a permis des changements structurels, organisationnels et symboliques importants dans la mise en scène des luttes politiques (Cardon, 2008, 2010). Par ce fait, les plateformes deviennent des lieux où se construisent de nouveaux espaces de visibilité. Espace de visibilité que les groupes extrémistes s'approprient pour construire de nouveaux procédés techniques, pratiques et communicationnels.

Certains réussissent ainsi habilement à orienter l'attention pour faire connaître leurs actions et positions politiques en ligne, tout en créant de nouvelles ressources symboliques. Une forme probante de ces nouvelles manifestations, qu'on accole généralement à l'expression « guerre de l'information », demeure la propagation de la propagande jihadiste. Nous avons vu que le web transforme les enjeux stratégiques de l'usage offensif de la communication. Alors qu'avec les médias traditionnels, les groupes extrémistes n'avaient que peu de contrôle sur la production médiatique les concernant, le web a marqué une nouvelle mutation dans l'économie de l'attention. S'ils peuvent maintenant produire et distribuer leur cause de façon indépendante, internet leur offre aussi la possibilité de tirer profit de phénomènes de viralité pour capter l'attention plus efficacement, plus longtemps et plus souvent.

Dans ce contexte de transformation, la diffusion d'idées extrémistes au sein des plateformes numériques est devenue un enjeu sécuritaire majeur. Les plateformes sont depuis quelques années mises à l'épreuve par la profusion de discours extrémistes en diffusion constante. Elles sont régulièrement accusées de jouer un rôle dans la radicalisation des individus et sont sommées d'être plus proactives dans la lutte anti-terroriste. Ce faisant, dans le discours public, la sécurisation d'internet est devenue l'une des conditions de la sécurité nationale, notamment pour se prémunir contre les attaques terroristes. Cela a favorisé l'éclosion de nouvelles initiatives et de nouveaux acteurs dans la lutte contre le terrorisme, en faisant intervenir massivement les plateformes numériques dans la régulation des flux informationnels jihadistes (Crosset et Dupont, 2018 ; Ganesh et Bright, 2020).

Devant ce nouvel horizon de luttes pour la visibilité, il est primordial de poursuivre et d'approfondir les recherches sur les dynamiques de l'apparence publique de mouvements militants susceptible d'user de violence politique. La question de la lutte pour la visibilité de groupes protestataires a depuis longtemps suscité réflexions, commentaires, analyses au sein de la sociologie des mouvements sociaux et des études en communication. Si la visibilité des groupes protestataires ne constitue pas un phénomène nouveau, il n'en reste pas moins que la visibilité ne peut être soumise à sa permanence dans le temps (Voirol, 2005b). La littérature a montré que la visibilité se transforme avec l'évolution des moyens de la générer, qui sont en progrès constant. Dans ce contexte, les médias sociaux vont permettre un ensemble de nouvelles formes d'actions et d'interactions (Thompson, 2005).

À notre grande surprise, bien que la littérature sur l'usage des technologies de communication par les mouvements sociaux soit imposante, moins nombreuses sont les études intéressées par la constitution mutuelle des technologies de communication et des militants. Pareillement, rares sont les travaux qui reconnaissent la participation essentielle des non-humains dans la composition de la visibilité médiatisée, préférant réfléchir aux effets de celle-ci sur les mouvements sociaux. Développons plus en profondeur ces différentes limites que nous chercherons à dépasser dans ce travail.

Si au départ, la sociologie des mouvements sociaux s'est intéressée au cadrage de l'action collective (Snow et al., 1984), négligeant l'importance des médias dans l'action collective, cette question a par la suite fait l'objet d'un examen approfondi (Gitlin, 1977, 1980 ; Gamson et al., 1992 ; Gamson et Wolsfeld, 1992). Les études sur les mouvements sociaux, extrémistes

ou non, ont régulièrement privilégié un instrumentalisme technologique. De ce point de vue, les technologies de communication sont présupposées neutres et ne sont qu'une simple ressource utilisée par les militants (Treré, 2019). Ces travaux décrivent ainsi la manière dont les technologies sont mobilisées pour atteindre certains objectifs particuliers comme le recrutement, la légitimation de la cause et l'intimidation des adversaires. Force est de constater que ces études adoptent la conception réductionniste selon laquelle les technologies de communication sont de simples transmetteurs qui véhiculent un message à une audience.

Au sein de la littérature, on assiste aussi à une compréhension fonctionnaliste des mouvements sociaux et des médias (Treré, 2019). Selon cette perspective, les technologies de communication ne sont cette fois-ci plus neutres, elles s'inscrivent en continuité par rapport aux mouvements sociaux. Elle rationalise par conséquent l'idée que les technologies de communication sont un supplément matérialisé des mouvements sociaux. Ce faisant, elle renforce l'idée que les mouvements sociaux précèdent les médias. Comme l'explique Treré (2019) « this functional reading of communication in collective action tends to almost completely disregard the role of media technologies as spaces for the creation and reproduction of specific social imaginaries, values, and world views » (p. 3). Dans cette perspective, l'auteur explique que les dimensions organisationnelles des mouvements et les *affordances* techniques ont tendance à être surestimées, au préjudice des dynamiques culturelles, émotionnelles et symboliques des mouvements sociaux.

Ainsi, jusqu'à présent les études sur la visibilité des groupes militants ont principalement perpétué le modèle binaire entre les humains et la technique. En leur attribuant une logique instrumentaliste ou fonctionnaliste, la question des reconfigurations entre les technologies de communication et des militants a été délaissée. Il faut dès lors dépasser ces conceptions, pour restituer la visibilité de groupes militants sur internet dans toute la complexité qu'elle dissimule. Étudier l'extrémisme en ligne sous cet angle permet l'évitement utopique ou dystopique dans lequel ces technologies peuvent facilement nous plonger ; à prendre au sérieux la matérialité ; et à penser l'activité technique des activistes au-delà des dualismes traditionnels (hors ligne et en ligne, ancien et nouveau média, homme et technique). Ainsi, il nous faudra éviter les raccourcis trompeurs qui cachent la complexité de la visibilité militante en ligne.

Dans la présente étude, l'accent sera donc mis sur les reconfigurations mutuelles entre les technologies numériques et les groupes militants, pour comprendre la complexité de la visibilité médiatisée. L'application du concept de symétrie (humain/non- humain, concepteur/usager) à la visibilité médiatisée de militants formera la base de notre travail. C'est lui qui nous nous permettra d'analyser la manière dont les assemblages humains et non-humains façonnent cette visibilité médiatisée. Cette étude exploratoire ne cherche donc pas à savoir ce que les médias font aux militants. L'intérêt porte plutôt sur les agencements entre des usagers militants et des technologies de communications. Des agencements, qui rappelons-le, conduisent à des innovations ou encore à des ruptures (Lievrouw, 2014).

Dans ce contexte, nous pouvons formuler la question centrale de notre thèse, qui sera explorée sous ses différents angles lors de nos analyses :

> ***Comment s'articule la relation entre un dispositif technique et un groupe qualifié d'extrémiste et quelles formes de visibilité cette co-constitution configure-t-elle ?***

Pour étudier cette reconfiguration mutuelle entre un dispositif technique et un groupe militant, notre recherche se penche plus spécifiquement sur l'usage de plateformes numériques par le groupe État islamique. Ce choix n'est pas fortuit. L'État islamique a révolutionné la communication de groupes insurgés et, plus généralement, la propagande, à plusieurs égards (Winter, 2018). L'État islamique a particulièrement brillé par l'ampleur et la sophistication de sa propagande. Fort de sa présence sur les réseaux sociaux, le groupe a attisé contre ses activités en ligne de vives hostilités. Par effet d'association, les réseaux sociaux ont été fortement critiqués en raison de la présence de ce type d'utilisateurs sur leurs plateformes. L'approche de ce cas conditionne la tâche qui nous attend : retracer les liens complexes, conflictuels, contingents, relationnels et productifs entre des dispositifs socio-techniques et des partisans de l'État islamique, à des fins de visibilité.

Ainsi, bien que la présente thèse recoupe certains aspects qui ont déjà été étudiés au sein de la sociologie de l'acteur-réseau, sa particularité sera d'orienter cette perspective sur un type d'usager peu étudié au sein de ce courant : un usager qualifié d'extrémiste. L'ANT a toujours porté son attention sur des utilisateurs peu violents et qui étaient généralement acceptés par le dispositif technique en question. Notre cas offre une autre lecture en s'intéressant cette fois à un type d'usager que les plupart des plateformes cherchent à exclure, en raison de la nature

violente et radicale qui le caractérise. Inversement, la sociologie de l'acteur-réseau, et plus largement les études en sciences et technologies n'ont suscité que peu d'intérêts au sein des travaux portant sur les mouvements extrémistes et leur participation en ligne. Il s'agit donc dans cette enquête d'observer la médiation technique entre un usager jugé indésirable et un dispositif technique, ce qui nous permettra de déterminer la manière dont ces relations sont forgées dans un ensemble de situations de conflits et de défaillances.

Notre objectif général est donc de comprendre la visibilité médiatisée de groupes qualifiés d'extrémistes, en tenant compte des reconfigurations mutuelles entre les technologies numériques et les groupes militants. À cette fin, nous nous concentrerons sur quatre sous-objectifs :

1. Décrire le rôle des humains et des non-humains dans le fonctionnement de la visibilité de groupes qualifiés d'extrémistes.
2. Identifier les récits et métaphores que les militants de l'État islamiques diffusent à l'encontre d'internet et des technologies de communication.
3. Retracer les difficultés, conflits et incertitudes associées à la relation entre les plateformes numériques et les usagers dits extrémistes.
4. Explorer les capacités de résistance du groupe face aux différentes stratégies de contrôle et d'interdiction qui visent à le déstabiliser.

Posons pour terminer les retombées attendues de la présente thèse. Premièrement, la démarche exploratoire proposée dans cette recherche permettra de mettre en lumière empiriquement la dynamique de visibilité de groupes extrémistes sur internet. En adoptant la perspective de l'ANT, ce projet participe à l'ouverture de « la boîte noire » de la médiation technique des plateformes numériques. Comme l'indique Callon (2006), l'ANT « est un chantier ouvert non une compréhension achevée et fermée » (p.13). C'est pourquoi revisiter la problématique de l'extrémisme en ligne à partir de l'ANT est porteur et novateur tant pour la criminologie que pour les études sur l'activisme en ligne et les études sur la sphère d'apparence de groupes radicaux.

D'une part, notre étude permettra d'appréhender les configurations complexes et changeantes qui se situent au centre de cette médiation technique. D'autre part, parmi les autres travaux intéressés par l'activisme en ligne (extrémiste ou non), notre démarche se distingue dans sa

manière de prendre explicitement en compte l'interrelation du technique et du social à l'ère des technologies numériques pour l'appliquer à l'étude de la visibilité. Nous espérons que notre étude pourra contribuer à problématiser davantage la visibilité en ligne de groupes extrémistes, et que cette problématisation servira de base pour des analyses ultérieures.

D'un point de vue méthodologique, notre étude est novatrice dans la mesure où son ethnographie digitale investit un terrain encore marginal dans ce type de démarche. Elle se démarque des méthodologies traditionnellement utilisées au sein de la sociologie des mouvements sociaux et de l'extrémisme en ligne. À notre connaissance, il existe peu, voire aucun, travaux ethnographiques sur la question de l'usage de technologies de communications par des groupes extrémistes. La méthodologie utilisée contribuera ainsi à documenter le champ de la sociologie digitale en expérimentant des pratiques de collecte de données et d'analyse de données. Elle permettra de poser les jalons d'une réflexion sur les terrains difficiles sur internet.

Nous pouvons également nous attendre à une contribution pratique non négligeable. L'analyse de l'apparence publique de l'État islamique sur les plateformes numériques permet d'aborder d'importants enjeux sociétaux et sécuritaires auxquels font face de nombreux pays, tels que l'apologie du terrorisme sur internet ou encore la diffusion de discours haineux et violents en ligne. Notre thèse permettra une meilleure compréhension de l'appropriation des plateformes numériques par les groupuscules extrémistes, les nouvelles guerres de l'information et l'effet du contrôle social numérique sur leur pratique.

Chapitre 4 : Stratégie et démarche méthodologiques

Ce chapitre présente la démarche méthodologique de notre enquête de terrain. Une démarche qui prend le parti d'intégrer une « sensibilité ethnographique » (Star, 1999) à la collecte et à l'analyse des données. La première section a pour objectif d'offrir un éclairage sur les choix méthodologiques embrassés pour répondre à nos questions de recherche. Elle situera les questions relatives à l'étude de cas et à sa description, ainsi qu'à l'enquête ethnographique appliquée à internet. Dans la seconde section, nous expliciterons notre terrain sur et par internet. La troisième abordera en détail les techniques d'enquête mobilisées. Ces techniques s'organisent autour de deux types de sources : l'observation en ligne et les sources documentaires. Cette section se terminera par une réflexion sur les aspects éthiques de la recherche en ligne. Dans la dernière section, nous exposerons quelques aspects de l'analyse de notre matériel.

4.1. Enquêter sur la visibilité en ligne : choix méthodologiques initiaux et sélection des approches

Pour rappel, notre objectif général est de renouveler le modèle de la visibilité médiatisée de groupuscules qualifiés d'extrémistes, en tenant compte des reconfigurations mutuelles entre les plateformes numériques et le groupe militant. Afin de faire de notre projet de recherche une étude empirique, nous ambitionnons de réaliser une étude de cas : celle de l'exploitation de plateformes numériques par l'État islamique. Étant donné que notre étude est exploratoire, ce projet privilégie une approche inductive. Pour répondre aux objectifs de notre thèse, la démarche qualitative nous est apparue comme étant la plus adéquate.

Bien que les groupes qualifiés d'extrémistes utilisent activement internet, leurs pratiques sont souvent mal documentées. Les méthodes utilisées ont effectivement eu tendance à privilégier l'analyse de contenu de grands ensembles de données (Ferrara, 2016 ; Gerstenfeld et al., 2003 ; Ghajar et al., 2016 ; Klausen, 2015 ; Qin et al. 2007) ou encore l'analyse de réseaux (Burris et al., 2000 ; Caiani et Parenti, 2009 ; 2011 ; Caiani et Wagemann, 2009). S'ensuit dès lors une perspective particulière des plateformes de réseaux sociaux ; ceux-ci ne seraient finalement rien d'autre que des sites remplis de textes et/ou de connexions entre des entités (Postill et Pink, 2012). Ces approches sont toutefois peu indiquées pour répondre à nos questions de recherche. Notre enquête a pour but d'ouvrir une voie différente : s'approcher des actions et des interactions entre les technologies et les usagers de l'État islamique tel qu'elles se produisent au quotidien, s'intéresser aux pratiques de visibilité *en train de se faire*, devenir familier avec les technologies et leurs usages. Il s'agit donc de faire ce que tous les ethnographes font : demeurer indépendant et à distance d'un terrain, tout en se rendant familier (Latour et Woolgar, 1996 : 23). La voie préconisée dans notre étude n'est toutefois pas celle d'une ethnographie au sens canonique du terme.

Un certain nombre d'omissions importantes, en partie dû à notre objet d'étude, fait de notre enquête une ethnographie partielle. Effectivement, en raison de la publicisation d'une idéologie radicale et violente, participer aux activités en ligne des militants de l'État islamique aurait causé de réels problèmes éthiques. Il serait toutefois malhonnête de notre part d'argumenter cet évitement à la participation sous le seul prétexte éthique. Assumons que ce qui constitue proprement notre intérêt, c'est de saisir notre cas en situation concrète sans en

altérer le cheminement. Relevons également que les technologies numériques concourent à délivrer une quantité impressionnante de traces numériques qui sont en elles-mêmes inédites et riches d'apprentissages. Au problème de partialité ethnographique, nous proposons une solution : plutôt que d'appliquer les canons de l'ethnographie traditionnelle, nous préférons appliquer une « sensibilité ethnographique » (Star, 1999) à l'observation de notre cas.

Par ailleurs, une autre difficulté de base concerne la manière de qualifier la population à l'étude. Enquêter sur les militants de l'État islamique implique que le chercheur se heurte à une diversité de vocabulaires qui se croisent et se rencontrent. Il y a les militants qui se décrivent comme des jihadistes. Et puis, il y a les pouvoirs publics, les plateformes numériques ou encore les internautes qui contribuent à définir ces acteurs en usant de propos normatifs. Ainsi, pour parer à ces qualifications normatives, notre posture cherchera à être la plus descriptive possible en faisant usage de termes comme activiste, militant, partisan ou encore jihadiste.

Avant d'expliciter plus avant le déroulement de notre enquête, nous commencerons par exposer brièvement les principes de méthode retenus pour étudier la visibilité en ligne de groupes impliqués dans des actes de violence.

4.1.1. Qu'est-ce qu'un cas ?

Nous avons stipulé que notre recherche repose sur l'étude du cas de l'État islamique et de son exploitation des plateformes numériques. Il convient d'emblée de se questionner sur ce qu'est une étude de cas. Malgré qu'elle revête des contours flous et mal définis en sciences sociales (Hammersley et Gomm, 2000 ; Ragin, 1992), les dictionnaires de sociologie l'associent à un objectif d'exploration, par où elle « tente de découvrir des problématiques nouvelles, de renouveler des perspectives existantes ou de suggérer des hypothèses fécondes » (Hamel, 1998 : 122). De surcroît, elle est généralement décrite comme « essentiellement descriptive, s'attachant à dépeindre toute la complexité d'un cas concret sans du tout prétendre au général » (Hamel, 1998 : 122). Cela amène l'auteur à faire le constat que la sociologie a traditionnellement traité l'étude de cas non pas comme une méthode, mais comme une *démarche*, résolument exploratoire. C'est avec une certaine condescendance que la sociologie a finalement convenu que l'étude de cas n'avait d'intérêt « qu'à titre de démarche exploratoire et celle-ci, pour donner corps à une étude, doit être confortée sinon régénérée par le moyen de

méthodes proprement dites » (Hamel, 1998 : 122). Or pour Yin (2003), on aurait tort de considérer l'étude de cas comme une démarche méthodologique embryonnaire à une recherche plus approfondie et généralisable.

Il faudra se tourner vers l'anthropologie pour retrouver les lettres de noblesse de l'étude de cas. Au sein de l'anthropologie, l'étude de cas, comme pendant de la monographie, est vue comme « une enquête empirique qui étudie un phénomène contemporain dans son contexte de vie réelle, où les limites entre le phénomène et le contexte ne sont pas nettement évidentes, et dans lequel ses sources d'informations multiples sont utilisées » (Hamel, 1998 : 123). L'anthropologie concède donc à l'étude de cas la possibilité de rendre observable la façon dont un phénomène se rapporte à son contexte. Notons par ailleurs que si l'étude de cas a pu être traitée avec un certain mépris en sociologie, nous ne pouvons affirmer qu'elle serait propre à l'anthropologie. L'auteur rappelle que celle-ci a occupé une place importante au sein de l'École de Chicago ou encore au sein de l'École de Le Play.

Toujours est-il que questionner ce qu'est un cas renvoie à une multitude de réponses (Ragin, 1992). C'est-à-dire qu'un cas peut concerner un objet limité ou non ; il peut être spécifique ou universel, déductif ou inductif, théorique ou empirique ou les deux. Ces différents usages et significations du cas auront des implications profondes sur la conduite de l'enquête (Latzo-Toth, 2009). Par exemple, des chercheurs comme Yin (2003) considèrent que l'étude de cas est illustrative ou probatoire au plan théorique et cherchent à tester ou corroborer une hypothèse. En conséquence, le cas se « développe déductivement à partir de la théorie mise en avant, de sorte que c'est elle qui en révèle les qualités comme cas démontrant sa valeur explicative » (Hamel, 1998 : 132).

Inversement, des auteurs tels que Gomm et ses collaborateurs (2000) donnent à l'étude de cas une sensibilité plus ethnographique. Celle-ci s'enracine dans une « description dense » (Geertz, 1998) des phénomènes sociaux observés et amène à l'élaboration de propositions théoriques. En ce sens, pour Gomm et ses collaborateurs, « les études de cas permettent de voir à l'œuvre – "in situ"- des chaînes de causalité et par suite, d'échafauder des théories » (Latzko-Toth, 2009 : 7). Elle est finalement ce qui permet d'ouvrir une boîte noire (Lacey, 1970 ; 1976). Elle renseigne, identifie et analyse les pratiques et les processus sociaux qui occasionnent le changement (Hammersley et Gomm, 2000). Cette posture n'est pas sans

rappeler celle de l'ANT et des STS qui postulent la nécessité d'ouvrir la boîte noire de tout fait scientifique ou d'artefact technique stabilisé (Latzo-Toth, 2009).

Dans cette conception, le choix de l'étude de cas se fait en fonction de ses qualités méthodologiques et non pas selon une théorie (Hamel, 1998). Latour (2006a) dit à ce propos que « le cas concret n'est donc que la réalisation d'une potentialité qui était déjà là » (p.222). Selon l'auteur, l'objectif n'est pas de basculer de la description à l'explication, mais de *prolonger* la description. Le choix du cas est donc crucial pour l'auteur, puisqu'il est ce qui génère de nouvelles connaissances. La position de l'auteur est à cet égard pour le moins tranchée : « une étude de cas qui a besoin d'être complétée par un cadre explicatif, c'est une étude de cas qui dès le départ a été mal choisie » (2006 : 209). L'auteur pointe que dans de telles circonstances, le cas ne serait pas porteur de nouvelles connaissances, étant donné qu'il ne ferait que confirmer ce qui est déjà connu ou ne comporterait aucune information au sens fort (Latzko-Toth, 2009).

Le choix de se rapporter à une étude de cas unique n'est donc pas anodin. Par rapport à nos objectifs, le cas se fonde comme une énigme à résoudre (Passeron et Revel, 2005). Il favorise une approche microsociologique *in situ* et élabore une description détaillée du phénomène (Hamel, 1997). En cela, notre étude de cas s'appuie sur l'observation des pratiques de visibilité en situation, s'efforçant de décrire les interactions en ligne quotidienne des militants de l'État islamique avec des humains et non-humains. Elle porte également une attention particulière au contexte socio-technique dans lequel cette visibilité se déroule et à ses stratégies. Enfin, elle s'intéresse aux conflits, aux crises et aux reconfigurations entre la technologie et l'usager de l'État islamique.

La question de la représentativité et de la généralisation des résultats d'une étude de cas est extrêmement débattue au sein des sciences sociales. Ragin (1992) résume que pour certains chercheurs l'étude de cas permet un autre type de conclusion que celle en recherche quantitative. Pires (1997) distingue par exemple deux niveaux de généralisation (empirique et théorique) et deux types de généralisation empirique (statistique et empirico-analytique). Les recherches ayant une structure ouverte comme les études de cas unique qualitatives, n'entraîne pas de généralisation empirique à proprement parler, mais produisent des généralisations analytico-théoriques.

Contrairement à « l'induction statistique » qui recherche des caractéristiques communes au plus grand nombre de cas, « l'induction analytique » a comme particularité de rechercher dans un cas concret les caractéristiques qui lui (ou leur) sont primordiales (ou les propriétés distinctives) et les généralise, hypothéquant que, parce qu'elles sont indispensables, elles doivent s'appliquer à d'autres cas analogues. Selon l'auteur, « la généralisation désigne alors les inférences analytiques faites à partir des observations sur la structure, les processus et le fonctionnement d'un système ou de la vie sociale » (p.59). Ainsi, l'étude de cas dépeint à maints égards d'autres cas, et la généralisation peut s'effectuer en ce sens qu'elle rend compte d'une « série de clés susceptibles de les [le chercheur ou le lecteur] aider à comprendre ce qui se passe ailleurs (généralisation analytique, plastique). Mais ce n'est pas le cas au complet et dans ses moindres détails qu'on généralise » (Pires, 1997 : 60). De même, Becker (2007) indique que le cas propose et élabore une généralisation qui se veut parcimonieuse. Cette « généralisation parcimonieuse » a principalement pour intérêt de permettre aux mots de garder leur spécificité. D'après l'auteur, la généralisation dans le cadre d'une étude en sociologie se doit d'être résolument prudente et mesurée.

4.1.2. Le statut de la description

Comme le soulève Hamel (1998), l'étude de cas est le prototype par excellence de la démarche descriptive. Plus généralement, la revalorisation du descriptif en sociologie ne s'inscrit pas dans une vision positiviste et épistémologique de l'objectivité de la connaissance (Quéré, 1992). Elle s'est au contraire érigée comme une alternative critique à la démarche hypothético-déductive, à l'explication causale et aux méthodes quantitatives. Adopter une démarche descriptive signifie un « retour aux choses elles-mêmes » (Quéré, 1992 : 141), en suspendant le jugement à son sujet (Becker, 2007). C'est là toute la valeur de la démarche descriptive ; elle participe d'une plus grande sensibilité aux dynamiques internes à l'œuvre dans les processus sociaux. Dans cette perspective, le monde social est regardé au plus près (Lemieux, 2018) ; il s'agit, comme les ethnométhodologues le recommandent, de « saisir les phénomènes dans leur site naturel d'occurrence » (Quéré, 1992 : 143). La description récuse ainsi le recours à toute pensée conventionnelle (Becker, 2007).

Quéré (1992) note que la démarche descriptive débouche sur deux soucis majeurs. Le premier est d'être informatif. En ce sens, l'analyse descriptive tend à rendre compte de la vie sociale dans toute sa richesse et diversité telle qu'elle s'orchestre en contexte de telle ou telle

situation, collectivité ou institution. L'objectif n'est donc pas de faire un compte rendu des corrélations entre les éléments d'un monde « objectif » ou de rapporter ses états à des facteurs causaux. Au contraire, il s'agit d'expliquer l'agencement de ce monde selon les acteurs d'une collectivité « en fonction des présupposés qu'ils adoptent dans l'"attitude naturelle" » (Quéré, 1992 : 146). Le second souci est ainsi de rendre justice à « la dynamique effective des processus sociaux, de la créativité des acteurs et du rôle des significations dans la structuration du monde social » (Quéré, 1992 : 142). En d'autres termes, faire usage de l'approche descriptive est une manière de « respecter l'intégrité des phénomènes sociaux » (Quéré, 1992 : 142).

Pour parvenir à des fins analytiques, les tenants d'une approche descriptive n'ont d'autres choix que d'innover sur le plan des techniques méthodologiques. Si nous avons soulevé des préceptes généraux, proches de la description ethnographique, il importe de préciser qu'il existe des styles de descriptions spécifiques à chaque tradition et école de pensée. Dans ce qui suit, nous nous centrerons essentiellement sur la description ethnographique traitée avec la méthode de l'ANT. L'un des impératifs méthodologiques les plus prégnants de l'ANT peut se résumer à recourir au principe d'internalisme (Lemieux, 2018). Dans son ouvrage *Changer de société, refaire de la sociologie*, Latour (2006a) préconise de « suivre les acteurs eux-mêmes, ou plutôt ce qui les fait agir, à savoir les modes d'existence » (p.342). Ce mot d'ordre « suivre les acteurs », devenu emblématique au sein de l'ANT, fait écho à la tradition interactionniste et à l'ethnométhodologie en sociologie (Lemieux, 2018). Il s'agit de « suivre les acteurs dans leur travail pour définir les situations qu'ils rencontrent plutôt que de leur opposer une définition extérieure de ces situations » (Lemieux, 2018 : 18). Suivre les acteurs consiste donc à se céder à toute volonté de discipliner l'enquêté (Latour, 2006a). En évitant de le faire coller à des catégories préétablies, l'enquêté est à même de pouvoir déployer son propre monde. Cette posture méthodologique n'est pas sans rappeler l'ethnométhodologie qui recommande à l'enquêteur de se départir de tout métalangage sociologique, plutôt que de lui attribuer continuellement « des intérêts, des calculs, des classes, des habitus, des structures aux acteurs sociaux supposé les marionnettes de la société » (Latour et Woolgar, 1998 : 25).

L'ANT reconnaît ainsi que la « mise en ordre » du social ne peut être monopolisée par l'enquêteur, mais doit être au contraire laissée aux acteurs eux-mêmes (Latour, 2006a). Il ne s'agit pas pour l'enquêteur d'établir un ordre défini par avance, mais de « trouver de l'ordre après avoir laissé les acteurs déployer toute la gamme des controverses dans lesquelles ils se

trouvent plonger » (Latour, 2006a : 36). Latour ajoute que se fier aux acteurs n'exclut pas pour autant l'exigence de l'ordre, de la rigueur et de la structure. Celle-ci est « seulement décalée d'un degré supplémentaire vers l'abstraction, afin que les acteurs puissent déployer leur différent cosmos, aussi contre-intuitifs qu'ils puissent paraître » (Latour, 2006a : 36). La démarche méthodologique de l'ANT consiste ainsi à suivre les actants qui participent à une chaîne d'action et à documenter les micro-épreuves et controverses qui prennent part à la solidification du réseau. De plus, comme les ethnométhodologues le recommandent, l'analyse ne se résout pas à celle de l'action déjà réalisée, mais s'étend au contraire à celles *en train de se faire*.

Une des critiques régulièrement formulées à l'égard de l'ANT est leur refus de prendre en compte « le temps long et le contexte "*plus large*", dans lesquels s'inscrivent les pratiques qui s'y déroulent » (Knorr Cetina, 1995, cité dans Hubert 2014 : 38). Il semble préférable d'admettre que si les tenants de l'ANT refusent de présupposer que certaines particularités historiques et structurelles puissent influer ou façonner les pratiques en cours, ils ne défendent pas un rejet total de toute *contextualisation*. Comme l'indique Hubert (2014) :

> Le contexte doit, selon Bruno Latour, être relocalisé au travers de différents médiateurs, qui en situation, contraignent, habilitent, permettent, interdisent ou cadrent l'action. Il peut également être réintroduit dans la description par les « *panoramas* » [Latour, 2006a] que dressent les acteurs, afin de se repérer et faire sens du monde dans lequel ils agissent. Dans cette perspective, le contexte demeure irréductible au point de vue de chacun. (p.39).

Cette démarche postule ainsi qu'il incombe à l'observateur de collecter les différentes contextualisations tirées des acteurs eux-mêmes. Sur cette question, nous divergerons minimalement de l'ANT. Outre les différentes contextualisations orchestrées par les acteurs, il convient de reconnaître qu'il puisse exister une certaine *grammaire*, une structure implicite (Boltanski et Thévenot, 1991) que le sociologue doit dégager par un travail d'observation. Tout en se bornant à l'ordre même de l'action, cela permet de rendre compte des formes de contextualisation qui peuvent renvoyer à des éléments du passé, à des formes institutionnelles ou encore à d'autres éléments mis en cause par les acteurs.

4.1.3. L'enquête ethnographique et internet

Les exigences fondamentales sur lesquelles se focalise l'enquête ethnographique sont de trois ordres : « recours à l'enquête empirique ; ouverture à ce qui n'est pas codifiable au moment de l'enquête ; accent mis sur l'observation directe, *in situ*, des activités ancrées dans un terrain » (Dodier et Baszanger, 1991 : 39). Mener une enquête ethnographique sur internet est particulièrement indiqué pour comprendre ce que les gens font réellement avec la technologie (Hine, 2000). Les premiers travaux qui ont appliqué les techniques ethnographiques à l'étude des interactions sur internet ont commencé dans les années 1990 (Baym, 1995 ; Paccagnella, 1997 ; Pastinelli, 1999 ; Pfaffenberger, 1996). Au cours des dernières décennies, ces travaux se sont multipliés, faisant émerger un corpus d'études ethnographiques sur les communautés en ligne, les sites, les plateformes et les pratiques des médias sociaux (Boellstorff, 2015 ; boyd, 2014 ; Coleman, 2016 ; Danet, 2001 ; Kendall, 2002 ; Marwick, 2013 ; Miller et Slater, 2000). Face à la diversité des terrains et des techniques pour mener une enquête ethnographique en ligne, une pléthore de dénominations est venue définir ces travaux. Parmi ceux-ci, on retrouve ; « ethnographie digitale » (Murthy, 2008), « cyber-ethnographie (Robinson et Schulz, 2009), « ethnographie sur internet » (Beaulieu, 2004), « ethnographie en ligne » (Paccagnella, 1997), « ethnographie des espaces virtuels » (Burrell, 2009), « netnographie » (Kozinets, 2010) ou encore « internet-*related* ethnography » (Postill et Pink, 2012).

Le dénominateur commun à toutes ces études est qu'elles transfèrent la tradition ethnographique comme instrument de recherche au sein d'internet (Hine, 2008). Pour Postill et Pink (2012), le web 2.0 a fait apparaître de nouveaux sites pour le travail ethnographique, de nouvelles pratiques ethnographiques et de nouvelles perspectives théoriques. Pour l'heure, il existe une série de conceptions concurrentes relatives aux approches ethnographiques sur internet. Berry (2012) en recense deux principales. Un premier ensemble de travaux veut rester fidèle à la tradition ethnographique classique et orthodoxe de l'anthropologie. La tâche de l'enquêteur consiste dès lors à porter attention aux relations entre les utilisateurs, aux interactions, aux rites et aux croyances. Cette conception insiste sur le fait d'envisager internet comme « un ensemble de microcosmes sociaux, de répliques en miniature de sociétés qu'il s'agit d'explorer » (Berry, 2012 : 37). Ces travaux marquent ainsi l'exigence de la participation et de l'apprentissage de codes, de procédures, de lois, de règles et de routines comme condition *sine qua non* à l'enquête.

Une autre voie consiste à se focaliser uniquement sur ce qui se passe à l'écran. Une conception, qui pour l'auteur, s'apparente davantage à l'ethnométhodologie. Dans cette conception, le travail de terrain devient celui d'une analyse des usages en ligne. Il cherche à mettre en relief « des activités qui constituent les routines des membres, qui sont autant de méthodes pour manifester et construire la réalité de la pratique étudiée » (Genvo, 2006, cité dans Berry, 2012 : 38). Dans une perspective épistémologique proche, un autre ensemble de travaux privilégie la posture de *lurker*. Ce faisant, ce qui doit être observé ce sont les textes lus et écrits par les utilisateurs, ainsi que les usages que font les utilisateurs de la technologie, sans intervention de la part du chercheur. Pour Coleman (2010), ces analyses ethnographiques sont méthodologiquement significatives, car elles permettent de faire sens des données – « internet memes, chatting, viral videos, and a stonishing cascade of comments that accompany this material – that may initially seem unsuitable for ethnographic analysis » (p.494).

Face au contexte d'enquête sur internet, plusieurs débats ont émergé, à savoir s'il y avait lieu d'innover sur le plan de la méthode. Une préoccupation qui, pour Pastinelli (2011), mérite d'être questionnée. S'il est indispensable de reconnaître les difficultés inhérentes au travail d'enquête sur internet, il importe de relativiser l'insistance prégnante d'un nouvel alignement méthodologique. À cet égard, l'auteure remarque que ce sont essentiellement « les perspectives disciplinaires et les façons d'envisager les rapports entre culture, société et technologies qui nous ont incités à voir ce contexte d'enquête comme radicalement différent de tous les autres » (p.36). Ainsi, plutôt que de plaider pour un renouvellement des méthodes lorsque l'enquête se passe en ligne, l'auteure rappelle que chaque terrain ethnographique a ses singularités. De surcroît, tout terrain représente un événement unique et confronte l'enquêteur à des difficultés et des contextes qu'il ne retrouverait pas ailleurs.

L'auteure insiste à ce titre sur la nécessité d'imagination, de créativité et de flexibilité dont doit faire preuve le chercheur afin que son enquête puisse se dérouler dans des contextes chaque fois uniques et singuliers. Dans la même veine, Hine (2000) soutient que l'ethnographie n'est pas une méthode normative, mais adaptative. S'inspirant de cette perspective, Postell et Pink (2012) insistent sur le fait qu'adapter les méthodes à de nouvelles situations « neither replaces long-term immersion in a society or culture, nor aims to prduce "classic" ethnographic knwoledge » (p.125). Cette flexibilité est ce qui permettra au contraire de révéler une compréhension profonde, contextuelle et contingente du phénomène étudié.

Enquêter sur le jihadisme en ligne : un terrain « difficile » ?

Une enquête ethnographique, qu'elle soit hors ligne ou en ligne, peut à bien des égards prendre la forme d'un terrain « difficile ». Pour certains terrains, la réalité difficile peut apparaître dès les premiers instants. C'est le cas par exemple pour les contextes de guerre, de conflits latents ou encore pour l'étude des groupes extrémistes. Ces terrains peuvent comporter une forte charge émotionnelle ou compromettre la sécurité physique du chercheur (voir par exemple, Romani, 2007). Pour d'autres, elle peut être identifiée a posteriori, au moment du traitement des données. Percevoir une difficulté et la manière d'y faire face est irréductiblement subjectif (Bizeul, 2007). Si l'estimation de la difficulté d'un terrain varie d'un chercheur à l'autre et d'un moment à l'autre, dans tous les cas elle fait transiter le chercheur sur une autre scène : celle de ses ressources personnelles et émotionnelles (Boumaza et Campana, 2007). Mais, qu'en est-il des terrains en ligne ? On peut être porté dans un premier temps à penser que l'écran protège l'enquêteur de toutes les formes de danger et de violence. Or l'écran feint la distanciation, plus qu'il ne la cultive. Les technologies numériques, en tant que média visuel (Nakamura, 2007), exposent le chercheur qui enquête sur l'extrémisme à l'hyper-réalité de la violence. Cette hyper-réalité de la violence est le fruit de médiatisations en chaîne, qui se superposent à la réalité. Il importe d'indiquer que cette violence « immatérielle » peut engendrer certaines difficultés émotionnelles pour le chercheur.

Les travaux de Baudrillard (2004) sur la violence faite aux images sont particulièrement éclairants. Pour l'auteur, il importe de distinguer deux types de violence. Il y a celle exercée par l'image directement, lorsque le chercheur est exposé à des « images intolérables » (Rancière, 2008). Au sein de ces images, tout doit être vu, tout doit être visible – c'est notamment le cas quand l'iconographie jihadiste met la violence à nu. Ces constructions visuelles rendent l'analyse difficile, risquant de la rendre impraticable. D'emblée, c'est la douleur ou l'indignation qui sont éprouvées. Le deuxième type identifié par Baudrillard est la violence du virtuel, dont le complice est la viralité. La violence du virtuel s'affranchit de tout ordre naturel. C'est la virulence qui prédomine. La violence ne s'exprime donc pas frontalement, mais à coups de contiguïtés, contagions et réactions en chaîne. Ce qui caractérise la violence du virtuel, c'est l'excès d'images jusqu'à saturation. Les difficultés éprouvées lors d'enquêtes en ligne s'inscrivent donc à différents degrés dans cette logique de fusion entre médium et message violent. Enquêter en ligne c'est s'exposer à la violence sans fin. Ces situations d'extrême violence malmènent les valeurs des chercheurs et le poussent dans des retranchements éthiques et émotionnels délicats. L'enquête, qu'elle soit en ligne ou hors ligne, s'exerce donc dans un contexte à la fois cognitif et émotionnel.

Les frontières d'un terrain en ligne

Dans son livre *Virtual ethnography*, Hine (2000) propose qu'internet soit compris à la fois comme une culture et comme un artefact culturel. En tant que culture, internet est un lieu où un ensemble de normes et de pratiques spécifiques se forment et se reforment. En tant qu'artefact culturel, internet est le produit d'une culture qui se façonne également en fonction des usages. En d'autres termes, internet est « increasingly entwined in people's live ; it is both an imagined space and an architected place » (boyd, 2009 : 26). Hine (2000) indique que les études sur internet se sont pour la plupart intéressées au statut culturel d'internet, délaissant ses propriétés à titre d'artefact culturel. Pour Hine, la combinaison de ces deux approches n'est toutefois pas exempte de difficultés méthodologiques. L'une de ces principales difficultés résulte du fait que les technologies numériques ont radicalement perturbé la notion de frontière.

Traditionnellement, les enquêtes ethnographiques ont toujours été menées au sein de sites physiques (boyd, 2009 ; Hine, 2000). L'attention de l'enquêteur se focalisait alors sur la culture, les peuples, les pratiques et les artefacts présents au sein d'espaces géographiquement délimités. Comme le note boyd (2009), cette approche était d'une certaine manière logique, puisque les premiers ethnographes ont essentiellement porté leur attention sur des populations à mobilité réduite. On peut dès lors comprendre qu'il y avait « a collective understanding that culture and people were contained by place » (boyd, 2009 : 26). Internet change toutefois la donne. Internet s'organise en dehors de toute délimitation et frontière : ce qui prime c'est l'interactivité (Hine, 2000, 2008). Comparativement à d'autres technologies, internet est difficilement localisable et délimitable. À l'évidence, le fait d'accéder à un monde hypertextuel et diffus démontre que l'espace géographique ne peut plus être ce qui définit la culture (boyd, 2009).

Dans ce contexte, Hine (2000, 2008, 2009) propose de dépasser une conception étroite de l'ethnographie. Il faut pour l'auteur se détourner de l'injonction d'un engagement prolongé du chercheur dans un espace social délimité. L'approche de Hine recommande au contraire que l'ethnographe mène son enquête au sein de différents sites. Ce modèle s'inspire de l'ethnographie multi-située mise de l'avant par Marcus (1995). D'après l'auteur, les années 1990 ont vu émerger une tendance en recherche qui consistait à adapter des modes anciens de pratiques ethnographiques à des objets d'études plus complexes, dont le terrain était plus difficile à circonscrire. L'ethnographie multi-située postule que les formations

culturelles ne peuvent se comprendre en se focalisant sur un seul site de recherche ethnographique ; celles-ci étant forgées dans plusieurs lieux différents. En cela, l'ethnographie multi-située se bâtît à partir de chaînes, de conjonctions et de juxtapositions de lieux et est portée par une logique explicite d'association et de connexion. En organisant l'enquête autour de connexion et non pas à partir d'un site délimité, l'ethnographie multi-située remet en cause l'holisme en ethnographie. À ce titre, l'auteur indique que « although multi-sited ethnography is an exercise in mapping terrain, its goal is not holistic representation, an ethnographic portrayal of the world system as a totality » (1995 :99). Les modes de constructions d'une ethnographie multi-située s'articulent à partir d'une gamme variée de stratégies. Parmi celles-ci, Marcus propose de suivre des personnes, des choses, des métaphores, des récits et des narratifs, des biographies et des conflits.

Si l'ethnographie multi-située a été particulièrement foisonnante dans les études sur les médias, les sciences et les technologies, notamment avec les travaux de Latour et d'Haraway (Marcus, 1995), elle occupe également une place de choix dans l'étude des technologies numériques :

> The emergence of multi-sited ethnography, conceived of as an experiential, interactive and engaged exploration of connectivity, is encouraging news for ethnography of the Internet. It offers up possibilities for designing a study which is based on the connections within and around the internet and enabled by it but not reliant on any one understanding of it (Hine, 2000 : 61).

Reprenant les préceptes de l'ethnographie multi-située, Hine (2000) recommande de voir le terrain sur internet comme un champs de relation (Hastrup et Olwig, 1997, cité dans Hine, 2000 : 60), où le hors-ligne et en ligne s'entremêlent de manière complexe. Cela suggère de suivre les connexions plutôt que de se référer à un site circonscrit qui préconise une période d'habitation. Plutôt que de privilégier l'holisme ethnographique (Hine, 2000 : 48), l'auteure soutient que le sens est produit contextuellement à travers « the circumstances in which the internet is used (offline) and the social spaces that ermerge through its use (online) » (2000 : 39).

Du fait qu'elle se rapporte malaisément à l'idée d'engagement sur un terrain unique, Hine soulève que l'enquête ethnographique sur internet serait par analogie un « flux de terrain » qui

se construit au fur et à mesure de l'enquête. L'enquête ethnographique sur internet peut donc ultimement porter sur la « mobility between contexts of production and use, and between online and offline, and it can creatively deploy forms of engagement to look at how these sites are socially constructed and at the same time are social conduits » (Hine, 2009 :11). Bien que l'enquête ethnographique soit marquée par des logiques d'association et de connexion, l'auteure rappelle que la clé de voûte de ce type de démarche reste l'immersion, « not necessarily through being in a particular field site, but by engaging in relevant practices wherever they might be found » (Hine, 2009 : 12).

4.2. Notre terrain sur et par internet

Formellement, notre terrain sur internet s'est déroulé de janvier 2017 à août 2018. Informellement, il s'est poursuivi à intervalles irréguliers jusqu'en 2019. Quitter un terrain qui demeure en tout temps accessible au chercheur, d'autant plus lorsqu'il s'avère aussi mouvant que celui des technologies numériques ; quitter ce terrain, disons-nous, représente un défi de taille. En raison de la nature interactive d'internet, nous avons effectué un suivi des connexions des militants de l'État islamique sur les différentes plateformes qu'ils exploitent. Par conséquent, notre attention ne s'est pas arrêtée sur un site en particulier, mais sur différents types de plateformes numériques – telles que les réseaux sociaux, les messageries cryptées, les sites web ou encore les *blogs*.

4.2.1. L'État islamique, Twitter et Telegram

D'entrée de jeu, précisons que notre terrain s'est réalisé dans un contexte différent de celui qui prévalait au moment d'élaborer notre projet de recherche en 2014. Jusqu'en 2015, les militants ont profité d'une large impunité sur les plateformes des médias sociaux. C'était l'âge d'or du jihadisme sur internet, c'était l'époque du « *lol jihad* » (Thompson, 2014). Au moment de commencer notre terrain, en 2017, la modération s'était davantage systématisée, poussant les partisans à ouvrir constamment de nouveaux comptes et à migrer vers des plateformes à l'accès plus restreint. C'est à ce moment on ne peut plus critique et kafkaïen pour les militants de l'État islamique que nous avons procédés à nos observations. Cela a incontestablement eu un effet sur notre enquête : les pratiques quotidiennes des militants allaient maintenant être examinées dans un environnement qui leur serait extrêmement hostile. De surcroît, les suspensions répétées ont considérablement modifié la dynamique du

terrain, au point de devenir un véritable défi méthodologique, comme nous le discuterons dans la section 4.3.1.

C'est en grande partie à travers l'observation de plateformes de réseaux sociaux et de messageries cryptées que le matériel a été collecté. Au moment de notre enquête, deux plateformes ressortaient particulièrement de l'activité en ligne des militants de l'État islamique, à savoir Twitter et Telegram. Twitter a longtemps été la plateforme de prédilection des partisans de l'État islamique. Cette plateforme présente effectivement l'avantage pour les partisans de pouvoir diffuser leur propagande à une large audience. Le renforcement de la politique de modération de Twitter a toutefois contraint les partisans à devoir exploiter des plateformes plus fermées et stables comme Telegram. Ces deux plateformes sont extrêmement différentes tant dans les usages qu'elles proposent que par les projets politiques qu'elles portent.

Twitter est l'une des plateformes de *microblogging* les plus populaires. Créée en 2006 par l'actuel PDG Jack Dorsey, au premier trimestre 2019 la plateforme ne comptait pas moins de 330 millions d'utilisateurs actifs par mois[43]. Lorsque l'utilisateur possède un compte Twitter, ce dernier est autorisé à publier des *tweets* de 280 caractères, rechercher et suivre des tendances, s'abonner à des comptes, *retweeter* et *liker* des *tweets* et envoyer des messages privés. Telegram est pour sa part une messagerie cryptée d'origine russe lancée en 2013 par Paval Durov (ancien directeur de la plateforme VKontakte –, l'équivalent du Facebook russe) et Nikolaï Durov. Contrairement aux grandes plateformes de la Silicon Valley, il s'agit d'une plateforme à but non lucratif créée dans le but d'échapper à la surveillance des autorités russes (Ermoshina et Musiani, 2012). Telegram offre à ses utilisateurs la possibilité de chiffrer leurs communications et d'envoyer des messages, des photos, des vidéos et des fichiers de n'importe quel type (doc, zip, mp3, etc.)[44]. De plus, chaque utilisateur est en mesure de créer des groupes pouvant contenir jusqu'à 200 000 personnes ou des chaînes qui permettent de diffuser du contenu à un public illimité. Notons que Telegram n'utilise toutefois pas le chiffrement de bout en bout par défaut. Si c'est le cas pour les conversations secrètes, les autres données de discussions seront stockées dans le *Cloud* de Telegram qui est réparti sur plusieurs serveurs à travers le monde.

[43] Voir « Nombre d'utilisateurs de Twitter dans le monde » : https://www.journaldunet.com/ebusiness/le-net/1159246-nombre-d-utilisateurs-de-twitter-dans-le-monde/
[44] Pour connaître l'ensemble des fonctionnalités de Telegram voir « Telegram FAQ » : https://telegram.org/faq

Si ces deux plateformes sont devenues les sites dominants de notre projet, c'est en raison de leur extrême popularité au sein des partisans de l'État islamique. La facilité d'accès n'a toutefois pas été similaire. Au moment de commencer notre terrain, nous avons immédiatement réussi à trouver des comptes Twitter pro État islamique. Les premiers comptes ont été repérés en parcourant les listes d'abonnés et d'abonnements de journalistes spécialisés sur les questions de jihadisme. Concernant Telegram, l'accès a été plus complexe et il nous aura fallu plusieurs semaines avant de rejoindre nos premières chaînes ou groupes de l'État islamique. Cette difficulté émane du fait que les chaînes ou les groupes sont principalement accessibles à partir de liens d'invitation que s'échangent les partisans de l'État islamique. C'est par le biais de liens publicisés par des militants de l'État islamique sur Twitter que nous avons réussi à accéder à nos premières chaînes Telegram.

Durant les premiers mois de notre enquête, c'est donc principalement sur Twitter que notre observation s'est concentrée. Nous étions effectivement en mesure de suivre quotidiennement une grande quantité de comptes : entre 50 et 100 comptes et 170 à 200 dans les meilleures périodes. Cependant, à partir du mois d'avril 2017 notre réseau sur Telegram est devenu plus consistant. Notre observation en a dès lors été considérablement modifiée. Nous passions maintenant la majeure partie de notre temps sur Telegram. Durant l'été 2017, nous suivions pas moins de 100 chaînes et groupes actifs en même temps. Que ce soit sur Twitter ou Telegram, nous avons fait usage de la technique dite de « boule de neige » (Rieder et Smyrmaios, 2012). Cela nous a permis de continuellement élargir notre réseau et de le garder actif malgré les suspensions régulières.

Nous avons toutefois remarqué au fur et à mesure de notre terrain que nous gravitions continuellement autour des mêmes niches d'utilisateurs. Ce qui les rassemblait : ils étaient anglophones et francophones pour la plupart, ils interagissaient entre eux et ils recréaient de nouveaux comptes, chaînes ou groupes après chaque fermeture par les plateformes de réseaux sociaux. Bien que notre réseau s'articulait autour des mêmes utilisateurs, il reste qu'il serait impossible de spécifier le nombre exact de personnes que nous avons suivies. Face à l'usage généralisé des pseudonymes au sein des partisans de l'État islamique, nous n'étions pas en mesure de connaître l'identité réelle des utilisateurs. Or, sur internet nous ne pouvons supposer qu'un compte est équivalent à un utilisateur. Certains utilisateurs peuvent avoir plusieurs comptes, tandis que d'autres comptes peuvent être gérés par plusieurs personnes ou

par des agents automatisés (Chu et al., 2010). De plus, il n'est pas toujours possible de reconnaître les personnes que nous aurions éventuellement observées auparavant dans l'environnement en ligne.

Parallèlement, tout au long de notre terrain, nous avons suivi d'autres plateformes numériques exploitées par les militants de l'État islamique. Quand les liens étaient mis à disposition, nous naviguions sur des *blogs*, des sites web pro État islamique et des sites d'archivages, tels que JustPaste.it et Archive.org. Nous avons également suivi les partisans sur d'autres plateformes de réseaux sociaux populaires comme YouTube, Facebook, Instagram, Google+[45] et Tumblr, et sur des plateformes plus marginales comme le réseau social Baaz et la messagerie instantanée riot.im. Ces observations étaient néanmoins plus ponctuelles, portant essentiellement sur Twitter et Telegram. L'ensemble de nos observations à la fois éparses et concentrées nous auront permis d'observer comment les partisans de l'État islamique utilisent et interagissent au quotidien avec des plateformes numériques ; la manière dont ils coordonnent leur visibilité à partir de plusieurs plateformes ; leurs interactions avec leurs adversaires ; ainsi que les effets de la modération et son appareillage socio-technique. Simultanément, nous avons pu suivre les récits et métaphores que les militants de l'État islamiques propageaient à l'encontre d'internet et des technologies de communication.

4.2.2. Me situer sur mon terrain

Je fais partie de ces jeunes adultes qui sont nés et ont grandi avec les technologies numériques[46]. Je comprends intuitivement ce qu'est Twitter, Facebook, YouTube, un *blog*, une messagerie cryptée ; ce qu'est un mème, un GIF, des tendances sur Twitter, un *like*, etc. Dans le cadre de ma recherche, je pouvais donc facilement m'adapter et apprendre de nouveaux usages en ligne. Mon utilisation des médias et des technologies s'alignait à bien des égards avec celles des jihadistes d'aujourd'hui ; consulter et publier des contenus, *liker* des publications, *retweeter*, cliquer sur des liens, naviguer sur différentes plateformes. Cela dit, il ne faut pas exagérer ce rapprochement : si j'utilise majoritairement les mêmes outils, je le fais différemment et pour d'autres raisons que celles des militants de l'État islamique. De plus, mon exposition journalière au média a peu en commun avec l'univers discursif et visuel des jihadistes.

[45] En raison d'une faible utilisation et de certaines failles de sécurité, la plateforme a été fermée en avril 2019. Voir : https://support.google.com/plus/answer/9195133

[46] Cette section abordant des enjeux personnels, elle est rédigée à la première personne du singulier.

Si j'avais une connaissance de la culture numérique, ce n'était pas le cas pour la culture jihadiste. Il importe de préciser qu'en raison de mon appartenance culturelle, je n'avais que très peu de repères en ce qui concerne les textes coraniques et certains préceptes de l'islam. Si mon intérêt était porté sur l'usager indésirable plus que sur le jihadiste en tant que tel, il n'en demeure pas moins que j'ai dû parallèlement approfondir mes connaissances théoriques sur le jihadisme et explorer le terrain avec prudence. Le fait que les utilisateurs que nous avons suivis exploitaient une série de références *mainstream* pour toucher un public plus occidentalisé, nous a néanmoins permis d'être dans une position plus confortable pour comprendre la culture jihadiste.

De manière plus générale, l'un des principaux défis de cette thèse est d'avoir été exposé par l'entremise de l'écran à une violence quotidienne. Si la violence ne constitue pas le registre à part entière du collectif, elle occupe toutefois une place non négligeable. Durant mon terrain, j'ai intériorisé quotidiennement les menaces répétées à l'égard de l'occident et de leurs ennemis, les images de mort et d'exécution, ainsi que celles de corps mutilés et démembrés par la guerre. Si dans ce contexte, l'intégrité physique du chercheur n'est pas menacée, l'image exhibe la mort et la violence dans sa dimension la plus réelle. Enquêter sur la violence pousse le chercheur dans ses retranchements à la fois affectif et éthique (Boumaza et Campana, 2007 : 11).

À propos de la dimension affective, deux moments clés méritent d'être explicités. Au moment de collecter les données, les émotions légitimement ressenties face à des contenus violents, telles que l'horreur, le dégoût, la révulsion ou encore la crainte, ont laissé place à un durcissement de mes standards et de mes normes morales. À force de visionner ces images, se présageait alors une sorte d'insensibilisation. Voir un cadavre, des corps décapités, des corps d'enfants bombardés, faisait partie de mon quotidien visuel. Néanmoins, penser qu'on s'habitue à l'intolérable n'est qu'illusion. Comme l'indique Romani (2007), l'objectif implicite de cette illusion est de pouvoir demeurer psychiquement disponible pour le reste de l'enquête. Il n'en reste pas moins que cette illusion puisse se délier à d'autres moments, c'est-à-dire lorsque vient la phase du traitement des données ou au moment de problématiser et construire l'objet d'étude. L'affectes m'a effectivement amenée à reconsidérer l'objet d'étude. Si au départ ma thèse portait sur le jihadisme, celle-ci s'est reconfigurée autour des technologies et des utilisateurs considérés comme indésirables. Cela montre en quoi les

réalités d'un terrain aux sensibilités délicates réservent au chercheur un « travail émotionnel » (Renzetti, 2012) qui lui incombe des ajustements constants.

Sur le plan éthique, que faire avec ces images d'extrême violence que les militants de l'État islamique nous livrent ? Exposer ce type de violence, c'est exposer des êtres anonymes aux corps mutilés. Cela conduit au développement d'un travail de réflexivité, en particulier quant à la légitimité scientifique d'une telle restitution. Il est certain que je ne pouvais exclure totalement ces contenus de l'analyse et de mon récit, étant donné que, comme les résultats le montreront, ils sont une partie non négligeable des stratégies et pratiques de visibilité des militants. J'ai donc décidé de transcrire cette violence le plus sobrement et le plus parcimonieusement possible.

4.2.3. Les limites d'un terrain sur et par internet

Internet offre des occasions inédites d'observation en temps réel et quasi-réel de groupes marginaux, autrement difficiles d'accès. Le fait d'avoir à portée de main une quantité aussi phénoménale de données vient cependant avec des contraintes, qui commandent une réflexion plus large sur l'utilisation d'internet pour la recherche en ligne (Buchanan, 2010 ; Hooley et al., 2011 ; Jones, 1998 ; Kitchin, 2014b ; Mann et Stewart, 2000 ; Manovich, 2011 ; Ruppert et al., 2013). C'est ainsi que l'essentiel de notre terrain s'appuie sur des données disponibles sur le web, sans démarche auprès des individus enquêtés. À partir de là, ce qui est empiriquement observable se modifie et incite le chercheur à penser les limites d'un terrain sur internet. Dans notre cas, nous avons recensé quatre limites à notre enquête.

Premièrement, la grande différence entre l'ethnographie traditionnelle et sur internet s'articule dans la substance et l'anonymat de l'enquêté. Jouët et Le Caroff (2017) remarquent à ce propos que si le champ d'observation est plus large et immédiat sur internet, il est ironiquement plus réduit que dans une ethnographie classique. Dans le cadre de notre enquête, ce que nous avons observé ce sont des traces numériques laissées par des internautes anonymes. Attardons-nous brièvement sur le concept de trace. Jeanneret (2011) définit la trace comme « un objet inscrit dans une matérialité que nous percevons dans notre environnement extérieur et dotons d'un potentiel de sens particulier » (p.61). Les traces numériques sont souvent des profils, des publications, des interactions, mais elles peuvent aussi être des traces d'usages et d'activités. Il est un fait qu'en basant notre observation

uniquement sur ces traces numériques, les catégories sociales, comme le sexe, le statut socioprofessionnel ou familial sont des dimensions qui ont été totalement absentes de notre enquête.

Cela est d'autant plus renforcé du fait de la nature de l'activité de notre population à l'étude. Les militants de l'État islamique ne divulguent pas leur identité réelle ou leurs informations personnelles. De telles pratiques signifient qu'il est difficile pour le chercheur de relier des données en ligne à des auteurs du monde réel ou de s'assurer que les propos représentent réellement les opinions de l'auteur. Sevingsson (2004) note que le fait que nous connaissons peu les personnes que nous étudions en ligne découle de deux aspects principaux. Premièrement, l'environnement numérique multiplie les occasions de manipuler son identité en ligne. Le deuxième aspect se réfère à un aspect déjà longuement discuté dans la littérature, celui qui consiste à dire que nous ne pouvons pas savoir si les internautes sont réellement ce qu'ils prétendent être sur internet. Une réalité qui se complique d'autant plus avec l'avènement des *botnets* qui tentent de plus en plus d'imiter le comportement humain.

Ne pas connaître l'identité réelle des internautes que nous observions ne constitue pas un problème pour l'atteinte de nos objectifs de recherche. Par contre, il fallait s'assurer que ces internautes soient réellement des partisans de l'État islamique. Si cette part de doute est quelque chose que le chercheur doit assumer, elle peut toutefois se réduire en passant de longues heures à observer ces acteurs en ligne. Durant notre enquête, en gravitant autour des mêmes internautes, nous avons appris à les connaître. Cette connaissance de certains internautes nous permettait de facilement les reconnaître lorsqu'ils réapparaissaient en ligne. Cela passait par leur pseudonyme, une photo de profil, une interaction avec un autre militant ou encore une manière de *tweeter* ou d'utiliser le dispositif technique.

La deuxième limite d'un terrain sur internet, est qu'il s'agit de données provenant pour la plupart d'entreprises privées. En d'autres termes, ce que le chercheur observe sur internet ce sont des « digital by-product of the routine operations of a large capitalist institution » (Savage et Burrows, 2007 : 887). Collecter des données numériques implique que nous devons tenir compte qu'elles ne sont pas objectives et ne sont pas intentionnellement produites pour le chercheur (boyd et Crawford, 2012 ; Gitelman, 2013 ; Marres, 2017). La conception d'après laquelle il s'agirait de données « naturelles » et objectives est essentiellement héritée des sciences computationnelles et de l'informatique (Venturini et al., 2014). Ces dernières ont eu tendance à survaloriser le pouvoir de vérité des données

numériques et de raviver le fantasme positiviste d'une « physique sociale » (Jurgenson, 2014). Prendre acte que les données numériques sont formatées par une longue chaîne de médiations qui échappe au contrôle direct du chercheur, permet de reconnaître leur artificialité. Cela n'exclut pas d'en faire un usage scientifique, mais requiert que le chercheur interroge les conditions de production des données numériques (Venturini et al., 2014). En d'autres termes, il s'agit de rendre manifestes ces « technological unconscious » (Thrift, 2004), pour que ne soient pas occultées les conditions de production de ces données. Pour que les traces numériques puissent être transformées en données, il incombe dès lors au chercheur d'effectuer des allers-retours permanents entre le dispositif technique et les traces produites par les utilisateurs.

Troisièmement, nous n'avons pas porté intérêt aux internautes et à leur vécu. Limiter l'observation aux traces numériques empêche d'emblée de cerner le contexte et les motivations des internautes. Certains éléments du phénomène ne sont effectivement pas observables à partir des sites de pages web ou de profils (Beaulieu, 2004). Par ce fait, les causes et les motivations de l'engagement des militants de l'État islamique sont des dimensions auxquelles nous n'avons pu accéder. Internet est un terrain formidable pour étudier des traces laissées par les internautes, mais ne comptons pas sur lui pour nous apprendre qui ils sont réellement. L'observation que nous avons menée ne livre que la dimension pragmatique des usages numériques. Elle ne permet pas de restituer le contexte plus large dans lequel ces usages et usagers s'inscrivent. Il est ainsi légitime de se demander quel type de savoir peut-être produit à partir de ces données ? Plutôt que de se rapporter à l'importance centrale de la causalité propre à la sociologie orthodoxe, l'étude des traces numériques fait valoir un tournant plus descriptif dans les sciences sociales (Savage, 2009 ; Savage et Burrow, 2007), tournant que nous avons expliqué dans la section 4.1.2.

Enfin, il importe de préciser que notre réseau de traces numériques ne représente qu'un point. Nos déplacements se sont situés uniquement sur internet, sans parcourir la totalité du réseau. Si dans le chapitre 5, nous décrivons comment l'État islamique produit des énoncés à partir de brochures distribuées aux « soldats des médias », ces données ont été collectées sur internet. La sphère physique nous était exclue, et ce, en raison des acteurs à l'étude. Pour des raisons éthiques et sécuritaires, il aurait été effectivement impossible de rejoindre des zones en conflit. Le médium est ici indispensable pour avoir accès à la communauté. Par ailleurs, nous ne prétendons pas avoir parcouru la totalité des lieux sur internet. Pour les terrains en ligne, il

faut se faire à l'idée, dès la conception, qu'il est impossible de sonder l'ensemble du réseau. Il a fallu sélectionner des internautes et des plateformes et en laisser d'autres se dérober à notre champ de vision. Cela implique des limites.

Premièrement, notre étude exploratoire ne peut être généralisée à toutes les plateformes du web. En tâchant de faire le suivi des connexions des militants de l'État islamique sur les différentes plateformes qu'ils exploitent, l'observation de différences dans l'utilisation des plateformes a permis de concentrer les efforts de recherche. En raison de la popularité de Twitter et de Telegram parmi les partisans de l'État islamique, ces deux sites sont devenus les sites dominants de notre étude. Nos observations sur d'autres réseaux sociaux, *blogs* et sites sont progressivement devenues plus ponctuelles. Rappelons que l'ambition de cette thèse n'est pas d'étudier Twitter ou Telegram, mais bien de décrire la guerre médiatique que l'État islamique mène en suivant les discours et métaphores concernant les technologies du web, les pratiques de visibilités et les pratiques de résistances. Il n'en demeure pas moins que des observations et analyses complémentaires sur d'autres plateformes numériques pourraient enrichir et approfondir les connaissances sur le phénomène à l'étude. Cela permettrait de détecter des similitudes et différences dans les stratégies de visibilité en ligne.

Deuxièmement, des internautes ont reçu moins d'attention que d'autres en raison de la barrière de la langue. C'est le cas des internautes arabophones, turcophones, russophones, etc. Ne pas prendre en compte ces acteurs ne nuit pas à proprement parler aux efforts pour établir l'existence de pratiques de visibilité, de savoir-faire et de compétences. Effectivement, en raison de la nature du médium, il n'existe pas de frontière nette entre les internautes arabophones, francophones, anglophones ou autres. Ce qui réunit ces internautes se présente sous une forme plus nette : 1) Le groupuscule opère sous la même idéologie ; 2) les militants sont regroupés autour de l'objectif de mener une guerre médiatique ; 3) conformément à ses ambitions déclarées de transnationalisation et de recrutement de combattants étrangers, l'État islamique et ses militants effectuent de nombreuses traductions des contenus propagés en langue arabe, au premier chef ses communiqués officiels. Ce travail de traduction effectué par les partisans de l'État islamique nous a permis d'avoir une compréhension plus générale des ambitions et spécificités du groupe. Rappelons que notre intérêt porte sur la construction et l'opérationnalisation de la visibilité des partisans de l'État islamique. Compte tenu de ce choix méthodologique, l'analyse systématique des contenus a été écartée au profit de l'observation des pratiques au quotidien. Cela dit, cette étude exploratoire ne prétend pas

avoir couvert ou décrit toute la gamme des transformations de la visibilité du collectif. Pour arriver à l'exhaustivité, des études complémentaires seront nécessaires.

4.3. La collecte de données

Les données qui façonnent ce projet proviennent de sources disparates, collectées pendant une période prolongée. La majeure partie du matériel a été collectée entre 2017 et 2019. Toutefois, certaines sources ont été recueillies dès 2014. Notre corpus s'est organisé autour d'un ensemble de données que l'on peut rassembler autour de deux grands types de sources – l'observation en ligne et le matériel documentaire. Ces documents sont de trois types : les documents produits par les protagonistes de l'État islamique ; ceux qui visent à faire « parler » les objets techniques ; et enfin les documents périphériques, qui comprennent les articles de presse et les documents législatifs[47]. Notre terrain a ainsi été alimenté par un va-et-vient constant entre l'observation et l'archive. Ce qui suit est une description des différents types de données auxquels nous avons eu accès durant notre terrain. Nous terminerons sur une réflexion relative aux enjeux éthiques de l'observation en ligne.

4.3.1. L'observation et la collecte en ligne

Le cœur empirique de notre recherche est une observation directe de l'activité en ligne des partisans de l'État islamique qui s'est étalée sur une période d'un an et demi. Notre observation en ligne s'est faite de manière clandestine et non participante[48]. En optant pour ce rôle, nous avons maintenu secrète notre activité d'observation aux militants de l'État islamique. C'est là un type d'observation qui a peu à voir avec l'observation participante, transparente et déclarée (Soulé, 2007 ; Peretz, 1998). L'observation clandestine, régulièrement classifiée comme une observation « à couvert », a ceci de particulier que le groupe « infiltré » n'est pas averti de la présence du chercheur (Soulé, 2007). Cette position, facilement endossable au sein des technologies numériques (Beaulieu, 2004 ; Thomsen et al., 1998), présente l'avantage d'avoir une grande liberté d'observation sans interférer dans les

[47] Une liste des documents collectés se trouve en Annexe 4 de ce travail.

[48] Notons néanmoins que quelques interactions ont été menées au cours de notre terrain avec des botnets de l'État islamique. Ces interactions se sont faites avec une dizaine de botnets sur Telegram. Il s'agissait toutefois d'interactions qui se limitaient à activer la commande du botnet. Hormis, nos faibles et rares interactions avec ces non-humains, notre observation a été non participante.

comportements des utilisateurs (Paccagnella, 1997). Nous avons ainsi pu suivre avec minutie les actions en ligne des partisans de l'État islamique sans en altérer leur cheminement.

Certaines plateformes se prêtent plus volontiers à la position de *lurker* que d'autres. À vrai dire, les plateformes qui ont constitué le cœur de notre enquête ne demandaient pas une réciprocité (c'est-à-dire faire une demande d'amitié) pour suivre les publications d'un compte. À partir d'un compte Twitter créé pour les besoins de l'enquête, nous pouvions suivre des comptes de militants de l'État islamique ouverts au public. Alors que dans un premier temps nous avons naïvement fait le choix de nous abonner aux comptes Twitter des partisans, notre stratégie a rapidement dû être changée. Au moment où nous avons commencé à suivre un nombre conséquent d'utilisateurs pro État islamique, notre compte Twitter a été suspendu.

D'un point de vue technique, recréer continuellement un nouveau compte aurait été irréalisable. C'est pourquoi nous avons fait le choix stratégique de suivre les partisans de l'État islamique en les regroupant au sein d'une liste privée. Comme l'explique la plateforme, une liste est « un groupe spécifique de comptes Twitter » qui affiche un flux de *tweet*s émanant uniquement de ces comptes[49]. Pareillement, Telegram ne demande pas de réciprocité pour rejoindre une chaîne ou un groupe. Toute personne qui dispose de l'application ou s'y connecte par internet est en mesure de rejoindre un lien d'invitation en circulation. Néanmoins, précisons qu'en rejoignant une chaîne ou un groupe, notre présence est confirmée à ses administrateurs.

Dans un tout autre registre, Facebook était quant à lui pratiquement impossible à utiliser pour la collecte de données. Hormis les rares cas d'utilisateurs qui laissaient certaines informations publiques, les profils des militants étaient habituellement fermés. Pour avoir accès à ces données, nous aurions dû faire une demande d'amitié avec notre compte personnel (la création d'un compte supplémentaire viole les conditions d'utilisations de Facebook) et recueillir le consentement des utilisateurs, puisqu'il s'agissait cette fois-ci de données privées. Nous avons donc limité notre observation aux seuls comptes qui étaient semi-publics. En ce qui concerne les autres plateformes qui ont fait l'objet d'une observation au moment de l'enquête (par exemple Tumblr, Baaz, riot.im, Instagram, YouTube), les informations

[49] Pour plus d'informations, voir « comment utiliser les listes Twitter », Twitter : https://help.twitter.com/fr/using-twitter/twitter-lists

collectées étaient toutes publiques et ne nécessitaient pas nécessairement de compte pour pouvoir les consulter.

L'observation au quotidien

Notre observation en ligne a consisté, pour sa plus grande part, à lire tous les jours les publications des militants jihadistes, à naviguer entre les profils jihadistes, à observer leur interaction, à prendre connaissance des disputes et des conflits avec leurs adversaires, et à suivre le phénomène plus largement, c'est-à-dire en lisant les publications sur Twitter de spécialistes de questions jihadistes. Lorsque nous étions impliqués dans l'observation et la collecte à plein temps, nous passions entre 30 et 50 heures par semaine en ligne. Une fois que nous avons eu une connaissance plus poussée du réseau et que nous pouvions facilement retrouver les utilisateurs exclus, notre temps moyen s'est stabilisé à 30 heures par semaine. Au total, nous estimons avoir passé environ 2 500 heures sur internet au moment de notre terrain. Nous avons suivi un total de 2 451 comptes Twitter et 1 738 chaînes et groupes Telegram. Ce chiffre est toutefois approximatif, puisqu'il n'a pas toujours été possible de noter chaque nouveau compte, chaîne ou groupe. Tous les profils, chaînes ou groupes que nous avons suivis étaient actifs au moment de la collecte. Nous avons essentiellement privilégié les publications et utilisateurs anglophones, francophones et multilingues (qui mélangeaient par exemple l'arabe et l'anglais). Par ailleurs, étant donné que les « traqueurs » de jihadistes sur Twitter font partie intégrante du quotidien en ligne des militants de l'État islamique, nous avons également observé ce type d'acteur.

L'observation et la collecte des données ont été difficiles pour deux raisons : l'instabilité du réseau et le volume considérable d'informations disponibles. Face au renforcement des suspensions, nos données étaient simultanément plus éphémères. La plupart des comptes que nous suivions sur Twitter étaient rapidement suspendus. Quant aux chaînes et groupes Telegram, si leur temps de viabilité était certes plus élevé, il n'en demeure pas moins que les suspensions faisaient également partie du quotidien des militants. Au moment de notre enquête, nous nous heurtions ainsi continuellement à des profils, chaînes et groupes suspendus.

Le caractère éphémère des données contraint le chercheur de diverses manières. Premièrement, il passe un temps considérable en ligne afin de retrouver les utilisateurs et les

chaînes ou les groupes suspendus. Une absence trop prolongée lui ferait courir le risque d'avoir des difficultés à reconstituer le réseau en ligne des militants de l'État islamique. Deuxièmement, il lui fait collecter les informations rapidement, avant que celles-ci ne disparaissent. Notons que nous ne pouvions jamais anticiper quand les suspensions allaient opérer. Prenons l'exemple de Twitter. Dans certains cas, le compte que nous étions en train de suivre disparaissait endéans les quelques minutes. Dans d'autres cas, cela prenait quelques heures. Et dans les cas les plus rares, plusieurs jours s'écoulaient avant que le compte soit suspendu.

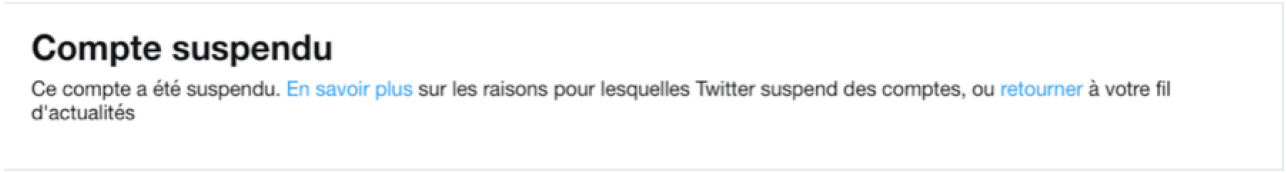

Figure 4.1. Message d'un compte suspendu sur Twitter

Une autre difficulté concerne la pléthore de données disponibles. Lorsque nous avons pénétré pour la première fois le monde numérique de l'État islamique, nous avons été déconcertés par la diversité des informations disponibles. Comment rapporter et classer les observations de façon systématique face à la multiplicité des contenus qui fusent et circulent de plateforme en plateforme ? Comment se mettre en phase avec un environnement qui change rapidement ? Quelle plateforme privilégier ? Qui suivre ? Définitivement, une période d'adaptation a été nécessaire afin de saisir la dynamique qui s'opère auprès des militants. Une fois encore, c'est l'observation sur la longue durée qui nous a permis d'affiner notre regard et notre connaissance du réseau. Au fur et à mesure de l'enquête, nous avons appris à connaître les routines des militants, les acteurs d'importance et les plateformes de prédilection.

Pour décrire ces pratiques quotidiennes qui produisent de la visibilité, l'observation en ligne doit s'accompagner d'un ensemble de techniques supplémentaires pour collecter le matériel numérique. Les données collectées de notre étude proviennent d'un archivage rigoureux et de notes d'observations compilées dans un journal de terrain. Sur le plan de l'archivage, nous avons cumulé plusieurs techniques selon les plateformes observées. Nous avons par exemple fait un usage prépondérant de la capture d'écran. Par ailleurs, quand cela s'y prêtait nous enregistrions les pages web, contenus et profils dans le logiciel Zotero ou sous format PDF. Nous avons dans des rares cas fait usage du logiciel payant Twitonomy qui nous permettait de

collecter automatiquement des *tweets* et d'avoir une analyse détaillée de l'activité de l'utilisateur.

Plateforme	Captures d'écran	Enregistrement dans Zotero	Enregistrement en format PDF
Twitter	805	2310 documents (comptes, *tweets* et interactions)	x
Telegram	13 450	x	511 chaînes et groupes
Tumblr	x	98 documents (pages Tumblr)	x
Instagram	141	x	x
Facebook	33	x	x
Baaz	95	x	x
Riot.im	10	x	x

Tableau 4.1. Types d'archivage selon les plateformes et nombre de documents archivés.

Face à la diversité des plateformes utilisées par l'État islamique et à la multitude des messages en circulation, il n'existe à ce jour aucun outil permettant de connaître la proportion des contenus et profils collectés par rapport à l'ensemble du web. Les difficultés à estimer la proportion des messages et des profils de l'État islamique sont documentées (Berger et Morgan, 2015). Par ailleurs, cette impossibilité a un faible impact sur notre démarche, dont la méthodologie ne vise pas la représentativité, mais à produire une description dense d'un

phénomène social (voir section 4.1.). Rappelons aussi que la collecte et l'observation sur ces différentes plateformes de réseaux sociaux n'avaient aucunement pour intention d'aboutir sur une comparaison systématique. Le but était de saisir les pratiques de visibilité des plateformes numériques et d'en faire un examen approfondi.

Parallèlement, nous inscrivions dans un journal de terrain des informations aussi diverses que des événements importants de la journée (opérations militaires, attaques terroristes) ; des discussions ordinaires ; des descriptions de leurs pratiques sur internet et de leurs innovations techniques ; des interactions entre des militants ainsi qu'avec des adversaires ; des informations éventuelles sur les internautes ; des descriptions de fonctionnalités informatiques et de structures de sites web ; ainsi que nos réflexions, sentiments et remarques. Ces informations ont été colligées dans le logiciel Word et comptabilisent plus de 600 pages de notes, de copier-coller de contenus et d'interactions et d'images éloquentes[50]. D'un point de vue technique, mener une enquête sur internet offre la possibilité pour le chercheur de mener son terrain depuis son bureau (Hine, 2000). Cette aisance lui permet de noter et de compiler ce qu'il observe à n'importe quel moment de la journée. Cette facilité peut toutefois rapidement se transformer en un piège pour l'enquêteur. On en conviendra : avoir la possibilité de noter tout ce qu'on observe, et ce en tout temps, peut mener le chercheur à ressentir de l'anxiété « at not writing down or recording 'the right things' during an ethnography » (Hine, 2000 : 22).

4.3.2. Les documents des protagonistes

La documentation produite par l'État islamique a constitué un deuxième type de source centrale pour notre étude. Les sources documentaires sont d'importants matériaux pour l'enquête de type ethnographique, en ce qu'ils « construct 'fact', 'records', 'diagnoses', 'decisions', and 'rules' » (Hammersley et Atkinson, 2007 : 121). Les documents fabriqués par les protagonistes nous ont essentiellement permis de suivre les récits et les métaphores que construisent les militants à l'égard d'internet et de son utilisation. Par ailleurs, cette documentation nous a fourni des informations cruciales en ce qui concerne les règles à suivre en ligne ; la structure de leur organisation médiatique ; les injonctions relatives à la production d'énoncés ; et les stratégies à adopter pour galvaniser les plateformes de réseaux sociaux. Le fait de s'intéresser aux sources textuelles et visuelles produites et consommées par les

[50] Notons qu'au début de l'enquête, nos observations étaient inscrites à la main dans un cahier. Ce qui s'est rapidement révélé être un défi impossible à relever, tant les observations collectées étaient abondantes.

militants de l'État islamique nous a permis d'avoir une lecture large et éclectique des pratiques de visibilités des militants. Ce matériel documentaire se distribue en deux grandes catégories.

Il s'agit en premier lieu de la documentation officielle et non officielle archivée sur le web par l'État islamique. Ce corpus inédit constitue une part cruciale de notre matériel collecté. Il existe une variété assez déroutante de documents distribués quotidiennement par les militants qui se sont avérés être d'une grande pertinence pour notre analyse. On y trouve des publications plus ou moins longues ; des tutoriels informatiques et de cybersécurité ; des pamphlets ; des infographies ; des statistiques ; des images ; de l'audiovisuel ; des livrets ; des mémos ; des brochures. Ces documents ont été collectés majoritairement sur les plateformes de réseaux sociaux et sur les sites web d'archive (JustPaste.it et archive.org) au moment de notre observation en ligne.

En second lieu, nous avons également eu accès à des mémos et des brochures produites par des instances officielles de l'État islamique, mis à disposition par le Combating Terrorism Center (CTC)[51]. Le CTC a mis à disposition du public une série de documents capturés par le département de la Défense des États-Unis lors d'une intervention ciblant le personnel de haut rang de l'État islamique du Khurasan en Afghanistan (Milton, 2018). Ils ont été obtenus par le ministère de la Défense entre 2016 et 2017 et été transmis au Combating Terrorism Center (CTC) qui les a publiés sur son site web en langue arabe et anglaise. Ces documents dateraient des années 2015 et 2016. Milton (2018) précise que malgré que ces documents aient été retrouvés en Afghanistan, rien n'indique qu'ils seraient spécifiques au bureau des médias de l'État islamique au Khurasan. Il s'agirait plutôt d'un matériel de formation générale pour tous les bureaux de presse de toutes les provinces de l'État islamique. Ces documents ont permis d'accéder à des informations inédites concernant les instructions générales données par les instances officielles du groupe à tous les bureaux de presse de toutes les provinces de l'État islamique. Ces documents permettent de restituer la manière avec laquelle le groupe construit et diffuse sa propagande. Une liste de ces documents figure en annexe 4 de ce travail et leur utilisation est précisée au chapitre 5 (section 5.2.1.).

[51] Le Combating Terrorism Center (CTC) est une institution académique et un centre de recherche de l'académie militaire des États-Unis.

4.3.3. Les sources documentaires pour faire « parler » l'objet technique

Le corpus de nos données ne se limite pas seulement aux protagonistes de l'État islamique. Ce qui nous intéresse, c'est à la fois le militant et le dispositif technique ou, dit autrement, c'est l'usager indésirable et le logiciel. Notre enquête a donc pour but de restituer le rôle des objets techniques qui participent à l'action. Ce point de l'enquête la rend plus délicate, puisqu'elle nécessite de faire sortir du silence l'ensemble des objets techniques qui peuplent la visibilité des militants de l'État islamique. Autrement dit, il s'agit de faire ressortir le travail invisible d'un objet technique forcément opaque. Reprenant les mots de Latour :

> C'est à cause de cette difficulté particulière qu'il faut inventer des stratagèmes pour les *faire parler* [les objets], c'est-à-dire pour leur faire produire des descriptions d'eux-mêmes, des *scripts* de ce qu'ils font faire aux autres – humains ou non-humains (2006a : 113-114).

Outre les observations menées sur les fonctionnalités informatiques utilisées par les militants, colligées dans notre carnet de notes ou au moyen de captures d'écran, nous avons dû recourir à des sources supplémentaires pour reconstituer l'action des utilisateurs et des logiciels. Pour ce faire, il nous fallait analyser plus en profondeur les fonctionnalités et les « logiques technico-culturelles » (Langlois et al., 2009b) des plateformes numériques. Nous avons ainsi lu et analysé une série de documents délivrés par les plateformes numériques qui détaillent certaines fonctionnalités, choix de conception et règles d'usage. Cette stratégie s'inscrit en droite ligne avec la proposition de Kirschenbaum (2003). Ce dernier suggère d'étudier les logiciels comme des « product of material environments » :

> These are material circumstances that leave material traces - in corporate archives, in email folders, on whiteboards and legal pads, in countless iterations of alpha versions and beta versions and patches and upgrades, in focus groups and user communities, in expense accounts, in licensing agreements, in stock options and IPOs, in carpal tunnel surgeries, and in the [former] Bay Area real estate market (to name just a few). (Kirschenbaum, 2003 : s.p)

Les logiciels sont donc le fruit de papiers, de spécifications techniques, de rapports qui sont facilement accessibles sur les sites ou les *blogs* des plateformes numériques. Nous avons ainsi porté notre attention sur cinq types de sources en particulier : le centre d'assistance, les FAQ (*frequently asked questions*), les conditions d'utilisation, les rapports de transparence et les *blogs* des plateformes numériques. Dans une moindre mesure, nous avons exploré la documentation produite par les développeurs (documentation API). Pour élargir notre

compréhension des technologies, nous avons par ailleurs consulté une série de *blogs* de programmeurs, ainsi que la presse et des sites web spécialisés sur les questions de technologie et de cybersécurité.

Recueillir les propos des propriétaires et des porte-parole de l'objet technique

Rappelons un fait. Les plateformes de réseaux sociaux à l'étude sont reconnues pour leurs efforts visant à obscurcir leur fonctionnement interne (Langlois et al., 2009). Elles fonctionnent généralement comme des « boîtes noires » et collaborent peu avec les chercheurs. Les raisons habituellement évoquées de cet obscurcissement sont d'ordre concurrentiel ou relatives à des problèmes de confidentialités (Kitchin, 2017). Les employés, les programmeurs et les propriétaires des géants du web sont donc difficilement accessibles pour approfondir les fonctionnalités techniques et la structure interne de la plateforme.

Toujours est-il que ces acteurs sont de grands communicants. Par ce fait, nous avons été en mesure de recueillir un ensemble de propos sur la manière dont ces acteurs combattent la profusion des contenus jihadistes au sein des plateformes numériques. Ces déclarations ressortent de trois sources documentaires principales : la presse, les réseaux sociaux et les communiqués. Pour rétablir une image plus positive de leur service, les fondateurs et porte-paroles des plateformes numériques se sont à plusieurs reprises exprimés dans les médias et sur les réseaux sociaux relativement aux mesures mises en place pour lutter contre les contenus terroristes en ligne. Ils ont aussi produit des communiqués plus détaillés sur ces mesures qu'ils publiaient sur le *blog* de la plateforme. En sus, nous avons également fait usage de l'audition de Mark Zuckerberg devant le Sénat américain le 10 avril 2018. Durant cette audition d'une durée de plus de cinq heures, le fondateur principalement interrogé sur le scandale Cambridge Analytica a également été amené à devoir parler de la modération des contenus sur sa plateforme. C'est dans ce contexte que Mark Zuckerberg a présenté à plusieurs reprises l'intelligence artificielle comme le futur de la modération des contenus et de la détection des fausses informations.

L'ensemble de ce matériel, ainsi que les données documentaires émanant des sites web des plateformes, nous permettra de répondre en partie au premier et deuxième sous-objectif,

mentionné ci-dessous. Ces sources documentaires nous permettront notamment de replacer les pratiques de visibilité du collectif dans le contexte socio-technique des logiciels. Par ailleurs, c'est par ce corpus documentaire que nous pourrons retracer la genèse et l'évolution des mesures anti-terroristes mises en place par les plateformes numériques.

4.3.4. Le matériel périphérique documentaire : Documents législatifs et articles de presse

Enfin, pour terminer, ce sont deux sources supplémentaires que nous avons ajoutées pour comprendre le contexte plus général des reconfigurations des plateformes numériques face à la prolifération des contenus terroristes en leur sein. Il s'agit premièrement d'un ensemble de documents juridiques, comprenant de nouvelles lois et de nouveaux règlements pour encadrer les technologies et favoriser la lutte contre le terrorisme. Ces nouvelles législations et règlements, issus de pays Européennes, nous permettent de reconstruire l'évolution des mesures anti-terroristes sur les plateformes numériques. Par exemple, on trouve les nouvelles législations qui ont émergé en France (la loi du 13 novembre 2014) et en Allemagne (la loi NetzDG en 2017), ainsi que le nouveau règlement européen relatif à la lutte contre la diffusion de contenus à caractère terroriste (2018).

En deuxième lieu, nous avons ciblé un ensemble d'articles de presse anglophones et francophones qui exposent les débats et actions qui ont émergé en matière de lutte contre la présence de l'État islamique sur internet. Pour suivre le déploiement de ces débats et actions, ainsi que leur évolution dans le temps, nous avons ciblé une période allant de 2014 à 2019. C'est en effet durant ces années que de nombreuses prises de conscience ont émergé en matière de lutte contre la présence de l'État islamique. S'il s'agit de documents additionnels, ces sources ont été essentielles pour mettre l'accent sur plusieurs moments clés de la mise en œuvre de dispositif de régulation au sein des plateformes numériques.

4.3.5. L'éthique de la recherche en ligne

Dès lors que l'on fait de la recherche en ligne sur des sujets sensibles, tels que la violence politique, les questions éthiques rattrapent rapidement le chercheur. Habituellement, les questions éthiques ne sont pas, ou peu, problématiques lorsque les données sur internet sont publiques et peu sensibles (Sveningsson, 2004). La situation se complexifie lorsque les données sont produites par des acteurs investis dans des violences politiques et des actes

qualifiés de terroriste. Par ailleurs, outre l'opportunité inédite d'observer les pratiques et les échanges des militants de l'État islamique sur internet sans en altérer le déroulement, la posture de *lurker* que nous avons adoptée nous a posé problème tout au long de notre cheminement. Elle s'avère en effet problématique lorsqu'on prend au sérieux le consentement éclairé des participants d'une recherche, le respect de leur vie privée et leur protection contre tout type de préjudice (Kleinman, 2004). Des préceptes primordiaux à toute recherche en sciences sociales qui, pour l'auteure, semblent s'estomper lorsqu'il s'agit de mener une recherche en ligne.

Au cours de notre enquête, plusieurs questions se sont ainsi imposées à nous. Avons-nous le droit de collecter librement des données accessibles au public à l'insu des militants ? Lorsque nous accédons à ce type de données, comment protéger l'anonymat et la vie privée des militants de l'État islamique ? Tenter de répondre à ces questions n'a pas été chose aisée. La diversité des contextes sur internet et la rapidité avec laquelle le dispositif évolue rend caduques toutes recommandations éthiques (Thoër et al., 2012). Comme le note Buchanan (2010), « the field of online research ethics is continually redefined by *and defining* the ethical challenges researchers experience daily vis-à-vis Internet environments and technologies » (p.88). En cela, selon l'auteur, il n'existe aucun manuel « clés en main » en ce qui concerne l'éthique de la recherche en ligne. Face au fait qu'il n'y a que peu ou prou de règles claires sur le plan éthique, pour Markham (2006, 2011), le chercheur devra non seulement être au fait des tendances et des débats actuels concernant l'éthique de la recherche en ligne, mais aussi s'engager dans une démarche réflexive et critique. Sans plus tarder, il nous faut éclairer notre démarche et les défis éthiques les plus épineux auxquels nous avons été confrontés.

La catégorisation a priori *publique* d'un réseau social nous a rapidement questionnés. Nous avons stipulé que les contenus auxquels nous avons eu accès ont tous été de nature publique. Lors de notre étude, il n'a jamais été question d'accéder à des contenus d'ordre privé. En revanche, le critère d'accessibilité des contenus en ligne est-il suffisant pour établir son caractère public ? Pour bon nombre d'auteurs, cette question est plus complexe qu'elle n'y paraît. En effet, ces derniers postulent généralement que la frontière entre la dimension publique et privée est floue et désuète (Beaulieu et Estalella, 2012 ; Bromseth, 2002 ; Convery et Cox, 2012 ; Eysenbach et Till, 2001 ; Markham, 2011 ; Pastinelli, 2011 ; Sveningsson, 2004). Selon Sveningsson (2004), ce n'est pas parce qu'un internaute publie une information

accessible, voire reconnue comme publique, qu'il accepte qu'elle se retrouve dans un autre contexte. Pour plusieurs auteurs (Baym et Markham 2009 ; Bromseth, 2002 ; Sveningsson, 2004), malgré la teneur publique de certains contenus, les internautes peuvent les percevoir comme étant privés.

Par ce fait, trancher entre le statut privé et public des informations recueillies s'avère peu utile pour orienter l'éthique de la recherche en ligne. Suivant Nissenbaum (2004), il importe plutôt de respecter « l'intégrité contextuelle » des données. Cela exige que la collecte et la diffusion d'informations obéissent aux normes (souvent informelles) spécifiques à un contexte social donné. Les militants de l'État islamique portent par exemple une attention particulière à ne diffuser aucune information personnelle. Dans ce cas de figure, il serait totalement inapproprié de révéler de telles informations dans un travail de thèse. Par ailleurs, l'information qu'ils diffusent est produite à des fins de propagande. L'une des normes implicites de la propagande est de rendre visibles et publics les contenus. Effectivement, l'information doit être suffisamment publique pour qu'elle puisse être consommée tant par les partisans que par les adversaires.

Toutefois, cette information est-elle suffisamment publique pour qu'elle puisse se passer du consentement des usagers ? Même si les informations que nous avons collectées sont prétendument publiques, elles témoignent d'une extrême sensibilité. Tout au long de notre enquête, nous avons considéré que nous n'étions pas seulement en contact avec des artefacts techniques et des avatars, mais avec des individus appartenant à un groupe jihadiste. À ce titre, les recommandations éthiques de l'AoIR indiquent que :

> A researcher cannot talk about discursive or physical participation in the online information sphere without acknowledging that this necessarily involves a person somewhere in the process—a person who is thinking and behaving within his or her own cultural and moral stances. (Markham et al., 2002 :5).

Traditionnellement, l'éthique recommande que les participants à une enquête soient informés. Nous avons décrit dans la section précédente les raisons méthodologiques qui nous ont poussés à choisir la posture de *lurker*. L'inégalité de la visibilité nous a néanmoins perturbés tout au long de notre terrain. Pourtant, recueillir le consentement individuel de l'ensemble des usagers nous a rapidement paru illusoire. Dans le contexte en ligne, il est extrêmement ardu

d'informer un à un les participants. En ce sens, nous rejoignons les conclusions de Dias (2003) quant à l'impossibilité d'obtenir le consentement éclairé, « because many on-line sites are openly accessible to the public » (p.33).

Lors de notre enquête, nous avons été frappés par le nombre important d'utilisateurs et le caractère mouvant de ceux-ci. Prenons le cas concret des groupes sur Telegram. Les groupes que nous avons suivis contenaient généralement des centaines de membres. La démographie du groupe évoluait constamment et rapidement, rendant obsolète toute tentative d'obtention du consentement de chaque individu. Dans un autre ordre d'idée, le processus aurait été d'autant plus complexifié par les multiples suspensions dont les militants font l'objet. Nous aurions ainsi été perpétuellement contraints de recommencer l'action, en tentant de repérer l'apparition de nouveaux utilisateurs.

Si le consentement éclairé est plus difficilement obtenu dans les contextes en ligne, Dias (2003) insiste sur le fait que « care needs to be taken to excercice the "fair use" of contributions to public forums that respects participants' privacy and protects them from harm » (p.33). Compte tenu du caractère sensible des contenus et de la vulnérabilité des participants de notre enquête, nous avons pris un certain nombre de précautions pour garantir leur anonymat. Pour commencer, nous avons décidé d'effacer toutes informations personnelles que nous aurions pu détenir. D'une certaine manière, les militants de l'État islamique nous ont facilité la tâche en fournissant peu d'informations à leur égard. Ces derniers travaillent énormément à sécuriser leur identité en ligne, rendant plus compliquées toutes tentatives de les identifier. En réalité, nous ne possédions que très peu d'informations personnelles sur les militants.

Notons que si les militants de l'État islamique dévoilent peu d'informations personnelles et utilisent des pseudonymes, cela ne garantit en rien leur anonymat (Markham, 2011 ; Donath, 1999). Dans certaines circonstances, il est effectivement possible d'associer le pseudonyme d'une personne à son identité hors-ligne (Roberts, 2015 ; Sveningsson, 2004). Afin de garantir au mieux la vie privée des participants, nous avons changé tous les pseudonymes de notre narratif. De plus, bien que la plupart des sites, chaînes ou groupes Telegram et profils de réseaux sociaux auxquels nous nous référons dans notre étude aient été suspendus, nous avons choisi de ne fournir aucun lien et nom de chaînes en référence à nos sources.

Par ailleurs, nous avons également dû prendre des précautions au moment de citer des extraits d'échanges et de contenus. Citer textuellement des propos en ligne permet de retrouver facilement des informations compte tenu du fait que les contenus sont systématiquement indexés par les moteurs de recherche (Beaulieu et Estalella, 2012 ; Bomseth, 2002 ; Eysenbauch et Till, 2001 ; Markham, 2011 ; Thoër et al., 2012). Notons que retracer les propos des militants de l'État islamique serait ardu, puisqu'ils ont largement été supprimés des plateformes numériques. Toutefois, cela n'empêche pas qu'ils puissent se retrouver sur d'autres sites web, comme des sites d'archivage par exemple. Pour minimiser les dommages potentiels, nous avons opté pour une utilisation limitée des citations directes. Lorsque nous y recourons, nous apportons des modifications mineures sans en altérer le discours. Nous avons par exemple corrigé l'orthographe et les mots en phonétique ou encore supprimé certaines parties du propos qui n'apportaient pas d'information pertinente. Pour chaque citation, nous avons ensuite vérifié à l'aide des moteurs de recherche qu'elle n'était plus consultable.

4.4. Analyse du matériel

Ce que nous cherchons à analyser, ce sont les reconfigurations mutuelles entre les militants de l'État islamique et les plateformes numériques. Ce faisant, nous n'analysons pas une population ou un espace spécifique, mais un assemblage de différentes entités humaines et non-humaines parsemé de moments de controverses, de conflits, d'échecs, de transitions et de moments stabilisés. Pour analyser notre matériel, nous avons constitué, d'après nos notes et notre cadre théorique, quatre dimensions clés de ces assemblages : 1) l'action ; 2) la relation ; 3) les micro-épreuves ; 4) les reconfigurations.

L'une des tâches importantes pour le chercheur est de mettre en récit le cas étudié, de raconter une histoire (Becker, 2007). Mais, comment rendre intelligible et communicable un cas, lorsque celui-ci émane de données à la fois vastes et éparses ? Comment trouver le seul bon « compte rendu » de la situation (Latour, 2006a) ? Certes, la littérature a largement exposé les défis méthodologiques de l'enquête en ligne. Toutefois, ceux de l'analyse sont généralement aux prises avec de nombreuses zones d'ombres. Comme le rappelle Star (2018), la recherche qualitative nécessite un travail laborieux de terrain et d'analyse. Face au changement d'échelle de l'enquête en ligne, « réduire ce volume de matériaux à quelque chose de gérable et d'analytiquement intéressant est une tâche difficile » (Star, 2018 : 8). Or, par quelle ficelle particulière analyser et interpréter qualitativement ces vastes ensembles de données sans être

noyée par la masse de détails ? Revenons brièvement sur notre itinéraire analytique qui, s'il a pour le moins été fastidieux, ne s'écarte pas d'approche traditionnelle.

Au vu de l'envergure des données collectées, nous avons trouvé pertinent d'utiliser dans un premier temps le logiciel d'analyse qualitative Nvivo 11. L'utilisation de ce logiciel a eu pour but de faciliter un premier travail de codification et de réduction des données. Cela nous a permis d'une certaine façon de faciliter la gestion du travail d'analyse. L'avantage de ce logiciel est qu'il permet une analyse manuelle des données collectées (Roy et Garon, 2013). En cela, il se rapproche de méthodes d'analyse plus traditionnelle et offre une certaine liberté au chercheur. De plus, il est possible de travailler avec différents types de données tels que du texte, du son, des pages web et de réseaux sociaux, des vidéos et des images. Indiquons d'emblée que ce logiciel a surtout été mobilisé pour soutenir nos analyses. Ce type de logiciel ne cherche pas à faire l'analyse à la place du chercheur. Plutôt, il procure « un espace structuré pour organiser ses idées » (Roy et Garon, 2013 : 163).

Nous avons codé dans une certaine mesure nos notes de terrains, documentations, pages web, images, publications et conversations des militants. Toutefois, ce logiciel s'est rapidement avéré décevant, en étant parfois trop élémentaire pour analyser l'enquête d'un terrain numérique. En raison de la nature diverse et variée de nos données, ces dernières nécessitaient des traitements différenciés difficilement exploitables avec le logiciel. Ce dernier ne nous permettait pas d'avoir la flexibilité qu'on retrouve dans des méthodes plus artisanales et manuelles. Prenons le cas de nos notes de terrain. Paillé (2011) rappelle que « les notes de terrain ne sont pas des données textuelles au sens que l'on pourrait en faire une analyse de contenu » (p.4). Ce faisant, ce matériel a particulièrement été ardu à traiter avec le logiciel Nvivo, dont son usage se prête plus facilement à l'analyse d'entrevues et à l'analyse textuelle et visuelle.

Face aux limites engendrées par ce type de logiciel, nous avons préféré dans un second temps un travail d'analyse à la main, ancré dans un processus d'écriture. D'une certaine manière, l'usage de logiciel d'analyse qualitative nous a permis de classifier nos données et d'avoir une vue d'ensemble sur ces dernières. Nous pourrions ainsi dire qu'il consiste en une première tentative d'appropriation de notre matériel analytique. Toutefois, l'analyse proprement dite a privilégié « l'écriture comme praxis d'analyse » (Paillé et Mucchielli, 2016 : 187). L'analyse en mode écriture est une méthode d'analyse qui :

> Au lieu de créer des entités conceptuelles, de générer des codes ou tout autre moyen de réduction ou d'étiquetage des données, l'analyste s'engage dans un travail délibéré d'écriture et de réécriture, sans autre moyen technique, et ce travail analytique tient lieu de reformulation, d'explication, d'interprétation ou de théorisation du matériau à l'étude. (Paillé et Mucchielli, 2016 : 187-188)

Si cela a eu pour effet de ralentir le processus d'analyse, ce travail permet « un contact plus charnel avec les matériaux et par conséquent des analyses bien incarnées » (Paillé, 2011 : 6). Comme l'indiquent Paillé et Mucchielli (2016), ce mode analytique valorise le texte suivi, plutôt que le recours à des thèmes et des catégories. Les auteurs ajoutent que « l'écriture permet plus que tout autre moyen de faire émerger directement le sens » (p. 192). Elle dépasse les stratégies qui ont recours à des systèmes de repérage et de classification des unités de sens du matériel analysé. Elle participe ainsi pleinement à la description des phénomènes observés, presque terme à terme.

En comparaison du logiciel d'analyse qualitative qui propose une expérience d'analyse codifiée et catégorisée, l'écriture analytique est plus flexible. Dans un premier temps, nous produisions sur une feuille ou un document dédié, des constats, des notes analytiques et éventuellement des catégories et des thématiques. Cette étape nous permettait de trier, supprimer, élaguer, ajouter les informations amassées lors de l'enquête. Ces constats et notes analytiques étaient constamment révisés, reformulés et enrichis au fur et à mesure de l'analyse.

Dans une seconde étape, nous procédions à la production de textes. Il s'agit d'un moment crucial dans notre travail d'analyse, puisqu'il a permis d'exploiter en détail les constats posés et de consolider notre regard interprétatif. Ce processus d'écriture a duré plusieurs mois et s'est soldé par de multiples relectures et enrichissements. Il nous a par ailleurs contraints à faire des détours, à explorer des pistes qui ont ensuite été renforcées ou abandonnées. Nous avons cumulé plusieurs séries de notes analytiques et de textes « pour épuiser les veines de la compréhension émergente » (Paillé et Mucchielli, 2016 : 195). Notre analyse a ainsi progressé « à mesure de l'écriture, de la réécriture et de l'accumulation, d'abord de constats, puis de plus en plus, de notes et de textes plus longs » (Paillé et Mucchielli, 2016 : 195). Inscrire le travail d'analyse dans la praxis de l'écriture, permet de formuler et d'ordonner de manière détaillée l'étude de cas.

PARTIE III :

La visibilité en ligne de l'État islamique

Chapitre 5 : Créer un théâtre d'action sur internet

Nous suivrons dans ce chapitre les premières tentatives qui visent à lier concrètement le dispositif technique et le collectif jihadiste. Il s'agira de saisir le programme d'action de cette nouvelle médiation technique. Nous verrons ainsi comment ce programme d'action définit un espace, des rôles et des règles (Akrich, 1990). Pour retracer cette histoire, nous sommes partis dans un premier temps de la manière dont l'État islamique se représente l'espace dans lequel il situe son action. En somme, nous analyserons le scénario, porté et énoncé par les membres de l'État islamique, qui engagent conjointement le collectif et le dispositif technique. Le chapitre se poursuit par la description d'une distribution des compétences entre des entités humaines et non-humaines, dont l'ensemble contribuera à la réalisation du programme d'action. À la suite de cela, nous ferons ressortir les différents appuis et règles qui permettront de faire fonctionner cet ensemble. Nous terminerons en décrivant comment le collectif théâtralise ses compétences techniques, ce qui contribue à montrer que le scénario n'est pas qu'un élément de langage, mais la concrétisation d'actions. Ces descriptions et analyses permettront de représenter le théâtre d'action sur lequel reposent les opérations médiatiques du collectif.

5.1. Élaboration d'un scénario pour internet

Commençons par une image. Un clavier d'ordinateur modélisé sous la forme d'une grenade à fragmentation prête à être déclenchée. L'image sera surplombée d'un slogan bien connu au sein de la sphère jihadiste : *half of jihad is media*[52]. La politique propre de ce type d'image consiste à enseigner aux spectateurs que l'espace numérique constitue une nouvelle ligne de front. Ce que les jihadistes associent plus formellement au jihad médiatique. Mais, qu'est-ce que le jihad médiatique ? Une première réponse nous vient directement du groupe. Dans un texte écrit par le Cheick Abû Hamzah al-Muhâjir[53], ce dernier parlait du jihad médiatique comme le « domaine du combat face aux médias sataniques qui ont dépouillé la communauté de son identité, l'ont fait dévier de la croyance authentique ainsi que de la voie de rectitude et ont ancré dans les esprits la base de la dépendance et de la défaite psychologiques » (p.29). Le jihad médiatique trouve toute sa raison en ce que « la chaleur des obus lancés par les médias est plus dévastatrice et plus dangereuse pour cette communauté et ses hommes que les flammes des missiles lancés par les avions » (p.29). Les « médias islamiques » (p.31) devront servir cinq objectifs :

- Défendre l'honneur des musulmans et leur dogme ;
- Élever la motivation des jeunes de la *umma*[54], et en particulier, des *mujâhidîn*[55] ;
- Dévoiler les mensonges des croyances et des mœurs des mécréants et des apostats ainsi qu'éclairer la *umma* au sujet de leur civilisation poubelle et le mensonge de ce qu'ils possèdent ;
- Sans oublier le fait de réfuter leurs attaques contre les musulmans et jeter l'effroi dans leurs cœurs ;

[52] Cette citation provient de l'égyptien Ayman al-Zawahiri, actuel chef d'Al-Qaïda, qui dans une lettre adressée à al-Zarqawi avait indiqué : « Mais en dépit de tout cela, je te dis que nous livrons une bataille, et que plus de la moitié de cette bataille se déroule sur la scène médiatique. Nous sommes donc engagés dans une bataille médiatique pour gagner les cœurs et les esprits des membres et, quelles que soient nos capacités, elles ne seront jamais qu'infimes par rapport à celle du royaume de Satan qui nous combat ». (*Lettre d'al-Zawahiri à al-Zarqawi, 2005*).

[53] Ancien chef d'Al-Qaïda en Irak après la mort en 2006 de son prédécesseur Abû Moussab al-Zarqaoui. Abû Hamzah al-Muhâjir a publié un texte dénommé « *Les chemins de la victoire* » auquel il a consacré une section à la « Préparation médiatique ». Le texte a été traduit en français en 2016 par la librairie Al-Himmah, organe de propagande de l'État islamique, et sera largement diffusé sur les réseaux sociaux et messageries.

[54] Dans la terminologie musulmane, la *umma* renvoie à la communauté des croyants. Elle dépasse toute appartenance tribale, ethnique et nationale au profit d'une solidarité entre les membres de la communauté religieuse.

[55] Les *mujâhidîn* sont ceux qui s'engagent dans le jihad. Souvent traduit par « guerrier de Dieu », selon le Oxford Islamic studies, à l'origine le terme n'est pas nécessairement lié à la guerre. Le terme a surtout été popularisé au début des années 1980 quand les *mujâhidîn* afghans ont combattu l'invasion soviétique en Afghanistan. Les *mujâhidîn* se considèrent comme des personnes pieuses qui combattent les injustices, notamment la domination étrangère, mais aussi contre des oppressions étatiques.

- Rapporter une image véridique de la réalité des combats qui ont lieu entre les héros de la religion et leurs ennemis ainsi que documenter l'héroïsme des jeunes de l'Islam, par crainte qu'il ne se perde ou qu'il soit voilé par les marchands de sang.

On peut noter que le jihad médiatique figure un combat idéologique entre le Bien et le Mal. Il recouvre une morale à suivre : l'exposition des Mensonges de l'ennemi et la restauration de la Vérité absolue. Cette dichotomie entre le Bien et le Mal est finalement un procédé assez commun dans les techniques de propagande (Almeida, 1995). Par ailleurs, les jihadistes avancent que la bataille médiatique date du temps du prophète Mahomet, où la poésie était utilisée pour combattre les forces ennemies. De cette valorisation de la guerre médiatique, s'en suit un ensemble de codification et de ritualisation pour la mettre en œuvre.

Dans un contexte où le jihad médiatique est rapidement devenu un point de passage obligé pour les partisans de l'État islamique, les appels à combattre sur le front médiatique se sont multipliés sur les plateformes numériques. On les retrouvait sous des formats à la fois audiovisuel, iconographique et textuel. Le collectif s'est en quelque sorte lancé dans une vaste campagne où il fallait armer le média, le rendre belliqueux, lui donner une forme quotidienne et maîtrisée, en le renouvelant à chaque instant dans le spectacle de la guerre. Se répandait alors l'idée que l'espace numérique est à envahir, de la même manière qu'une armée occuperait un territoire. Cette idée s'articule assez clairement dans ce passage d'un communiqué non-officiel diffusé sur Telegram par un organe de propagande pro État islamique :

> We praise the Islamic state media knights and supporters, blessings upon their jihad and struggling over the Facebook Twitter and YouTube sphere rather than the other communicating sites. Today the Islamic State supporters battle on media is not less in it is importance than the military battle and we specialize #invasion units, #upgrading knights and #publishing as you were to the kuffar beliefs serviling and with your words and fourtanating stability and sacrificing for your islam religion[56].

Face à ces objectifs guerriers, l'espace numérique allait rapidement se fondre dans une esthétisation de la violence. L'usager devient un *mujâhidîn* des médias. On le représente régulièrement portant un uniforme noir, masqué et anonyme. Il est assis derrière un ordinateur en train de taper sur un clavier. Il est seul, pour rappeler que l'action se mène

[56] Communiqué non-officiel « *The media is yours* », téléchargé sur Telegram le 22 mars 2017

individuellement. Ordinateurs, matériels informatiques et logos de réseaux sociaux se mêlent quant à eux à l'étendard de l'État islamique et aux kalachnikovs, un classique du jihad. Créant leur économie de l'attention sur un ensemble de technologies occidentales, les militants de l'État islamique mettent en scène les fondateurs des grands réseaux sociaux dans des représentations macabres, violentes et menaçantes. Voilà donc le travail d'esthétisation de la violence sur internet auquel les partisans de l'État islamique s'adonnent. Il sert à formuler une mythologie de l'objet technique qui contient le germe du combat. Ici, le terme mythologie renvoie à un ensemble de pratiques et d'activités d'une culture particulière, « un *accord* au monde […], tel qu'il veut se faire » (Barthes, 1957 : 230).

Nous voyons ainsi plus distinctement comment le dispositif technique est devenu une rationalisation opérationnelle. Plus qu'un simple moyen de communiquer, les moments en ligne doivent s'accompagner de ruses et de stratégies belliqueuses. Cette emphase sur le combat dévoile instantanément la marche à suivre sur le réseau et la relation qu'entretient l'État islamique avec le dispositif technique. Cette prise en main du dispositif technique nous montre quelque chose que nous devrions savoir à propos de la technique : il existe de nombreux « régimes d'engagement » (Thévenot, 2006) au cœur d'internet. En cela, pour Dodier, tout objet technique est porteur d'un *éthos* au sens wébérien, du fait que « les personnes engagées dans une activité technique ne mobilisent pas seulement une compétence d'adaptation (…), mais également une capacité à agir selon une visée qui, le cas échéant, peut aller contre le fonctionnement de l'ensemble, et l'enrayer, ou le déplacer » (1995 : 191).

D'une autre manière, elle mine les scénarios de ses concepteurs, en valorisant une activité technique qui s'écarte des usages prévus par les plateformes numériques. La synthèse des valeurs jihadistes et d'une technique occidentale superpose aux réseaux sociaux des objectifs militarisés, exclus de la conception d'origine. D'usages conviviaux et interactifs promus par les plateformes numériques, nous passons à des usages qui valorisent l'hostilité et le conflit. Ce fossé rappelle que les dispositifs techniques ne sont jamais complètement concrétisés et continuellement reconfigurés par les usages qui en sont faits (Dodier, 1995). Par ailleurs, cela ne signifie pas pour autant que les partisans jihadistes se limitent à allier uniquement des pratiques hostiles à leurs usages. Au contraire, les partisans effectuent un va-et-vient constant entre le monde de la convivialité à celui de l'hostilité.

Figure 5.1. Image non-officielle qui incite les partisans à mener le jihad médiatique sur YouTube, Facebook et Twitter diffusée sur Telegram en 2017.

Figure 5.2. Image non officielle faisant des menaces explicites à l'encontre de Jack Dorsey, co-fondateur et PDG de Twitter diffusée sur Telegram en 2017.

À ce stade, nous pouvons dire que le collectif accorde un statut instrumental au dispositif technique. Tout culmine effectivement dans l'idée que les technologies numériques constituent un moyen de consolider la guerre médiatique. Le jihad médiatique en ligne concède un jeu d'articulations fines pour arriver à une configuration particulière du dispositif technique et obtenir un résultat spécifique. Face à cette mise en rapport entre guerre et technologies numériques, on comprend rapidement que le groupe n'expose pas le spectateur à la convivialité, mais à un combat qui se joue maintenant au sein des plateformes. D'un mot : les jihadistes allaient faire d'internet un espace militarisé. Cette manière de s'inscrire dans le dispositif technique a ceci de spécifique que l'utilisateur jihadiste est pris dans des batailles, a des adversaires et se bat pour vaincre.

5.2. Mener l'action par des collectifs hybrides

Maintenant que nous avons le scénario qui engage conjointement le jihadiste et le dispositif technique, nous pouvons nous demander : qui assure la réalisation de ce programme d'action ? C'est à cette question que nous tenterons de répondre dans cette section. Nous verrons que ce « réseau technico-jihadiste »[57] est principalement organisé autour de trois pôles : 1° Le pôle des professionnels des médias qui produisent des énoncés officiels et certifiés ; 2° Le pôle technique qui regroupe une panoplie d'actants tels que l'ensemble du matériel médiatique, des *botnets* ou encore des spécialistes en cybersécurité ; 3° Le pôle des internautes qui comprend les partisans qui ont rejoint la guerre médiatique en relayant et produisant des énoncés. Dans cette section, nous nous demanderons comment cet ensemble coordonné d'acteurs hétérogènes participe collectivement à la production, à la circulation et au maintien du flux informationnel pro État islamique.

5.2.1. Les spécialistes des médias

Parler de la « structure médiatique » de l'État islamique n'a jamais été notre intention, supposant que cela ferait partie d'un autre projet de recherche. Cependant, lors de notre enquête, nous avons rapidement rencontré des contenus hautement professionnalisés. Ouvrir

[57] Cette appellation s'inspire directement de Callon (1991) lorsqu'il parle de « réseau technico-économique (RTE) » pour signifier « un ensemble coordonné d'acteurs hétérogènes : laboratoires publics, centres de recherche technique, entreprises, organismes financiers, usagers et pouvoirs publics qui participent collectivement à la conception, à l'élaboration, à la production et à la distribution-diffusion des procédés de production, de biens et de services dont certains donnent lieu à une transaction marchande ». De la même manière, nous utilisons cette appellation pour indiquer les nombreuses entités incluses dans ce réseau qui permettent la production et la circulation des énoncés.

la « boîte noire » de ces contenus, a remis en jeu toute une série de lieux et d'acteurs invisibles à l'observatrice et pourtant cruciaux dans le cadrage de l'action médiatique et la distribution des contenus en ligne. Si cette manie de l'État islamique de documenter tout ce qu'il se passait sur le terrain militaire et au sein des zones qu'il contrôlait était totalement visible à l'observateur, le processus et les acteurs en arrière lui étaient totalement invisibles. Pour comprendre comment ces contenus étaient produits, nous avons eu accès à différents mémos et brochures qui comprenaient des instructions fournies par le *Diwan du Média Central*[58]. L'ensemble de ces documents, mêlés à nos observations quotidiennes sur internet, nous aura permis d'observer que la production des contenus officiels de l'État islamique était hautement hiérarchisée et professionnalisée.

Distribution des rôles

Pour élaborer sa campagne médiatique, l'État islamique a maintenu une structure hiérarchique avec des porte-paroles et de centres médiatiques officiels. Le Média Central dispose de plusieurs institutions médiatiques qui diffusent les événements se produisant sous l'autorité du Califat autoproclamé. Ces institutions comprennent la Fondation Al-Furqan, le Centre médiatique Al-Hayat, Al-Furat, Al-l`tisam et la librairie Al-Himmah. Le Média Central dispose également du journal hebdomadaire Al-Naba, de l'agence de presse A`maq[59] et de la radio Al-Bayan. Pour donner toute son ampleur à son récit, autant dire sa propagande, ces différents centres médiatiques ont excellé à fournir des inscriptions diversifiées, se regroupant sous quatre grandes catégories : texte, audio, visuel et audiovisuel. Le Média Central, aura quelques plateformes en ligne pour diffuser les contenus, tels que la chaîne Telegram Nashir, le site web Nashir, la chaîne Telegram du centre médiatique Al-Furat, ainsi que divers comptes, chaînes, sites et applications qui publient dans différentes langues. À côté des centres médiatiques officiels de l'État islamique, chaque province contrôlée par le groupe a son propre Bureau des médias. Ces derniers ont pour vocation de distribuer le matériel officiel de l'État islamique (ce qui est associé à la diffusion interne) et de documenter tout ce qu'il se passe à l'intérieur du territoire.

[58] Il s'agit de l'organisation centrale chargée des opérations médiatiques du groupe.

[59] Le statut d'indépendance de l'agence de presse A`maq a longuement été questionné. Comme l'explique le Romain Caillet, à ses débuts l'agence de presse est apparue indépendante de l'État islamique. La particularité d'A'maq est qu'elle joue sur la neutralité en excluant tout langage partisan et triomphaliste. Qu'il soit indépendant ou non, il est toutefois apparu dans les différentes broches de l'État islamique comme un média de choix, au même titre que d'autres entités médiatiques comme Al-Naba et Al-Bayan (Milton, 2018). Cela atteste par conséquent une premier lien entre le Bureau Central des Médias et l'« agence de presse » A'maq (voir notamment le document « *Responsabilities of Media Offices towards A`maq agency* » : https://ctc.usma.edu/app/uploads/2018/08/Responsibilities-of-Media-Offices-towards-Amaq-Agency.pdf).

C'est un fait : les documents produits par l'État islamique démontrent une volonté d'exercer un contrôle strict sur la production de matériel médiatique. Au cours de son histoire, le groupe a misé sur une organisation bureaucratique pour produire ses contenus. Il y a une hiérarchie, des règles, des sanctions et des normes de productivité à remplir. Chaque publication du Bureau des médias doit recevoir l'accord d'instances supérieures avant d'être publiée. Par ailleurs, les Bureaux des médias sont également contraints d'envoyer au comité de Surveillance des médias leurs statistiques mensuelles sur le nombre de supports médiatiques produits[60]. Les brochures insistent aussi sur l'importance d'évaluer les professionnels des médias. Récompenser les meilleurs et critiquer les mauvais, telle était la devise. Les vertus d'un contrôle strict sur le processus éditorial sont une manière pour le groupe d'assurer la crédibilité et d'éviter la discorde au sein du groupe. On ne pourrait mieux caractériser l'impératif de suivre les consignes par le passage suivant :

> And know that the publication of any material in a random way, will result in the loss of credibility of the wilayah media and the credibility of those materials that were published in an unofficial method, causing the spread of rumors, gossip, and questions.[61]

Concernant internet, les instances officielles de l'État islamique ont tout autant été extrêmement strictes. Les Bureaux des médias ont pour obligation de se conformer aux restrictions et directives émises par le Média Central. Auquel cas, le Média Central se réservait le droit de lui restreindre l'accès.

> Exterior publishing (via the Internet) is the responsibility of the Central Media exclusively. The media bureaus of the wilayah are authorized to publish according to central restrictions and guidance that are executed under the supervision of the Media Monitoring Committee of the Diman of Media. And it (the Central Media) has the right to withdraw that authority from the wilayah and deprive it access to this platform if it (the wilayah) doesn't abide by the media policy according to the restrictions and directions put by the Central Media Diwan[62].

En ce qui concerne le personnel des médias, il leur est vivement déconseillé de créer des comptes de réseaux sociaux ou des sites web pour d'autres objectifs que celui de diffuser les contenus officiels de l'État islamique :

---

[60] À ce propos, voir Annexe 2 *The Table to Evaluate Video Releases* et Annexe 3 *Top 10 Video Releases for Month of Rajab.*
[61] Brochure « *Clarification Regarding the Media of Islamic State* »
[62] Brochure « *The Essential Duties of the Media Mujahid* »

> We want you to order all media personnel not to open any accounts, websites, channels, or institutions and have them serve as exclusive publishing platforms for what they document, and to close all the channels, accounts, and institutions that they have opened for that purpose.[63]

Tout était donc fort bien réglé. Ces instructions fournies par le Média Central montrent que l'État islamique cherche à exercer un contrôle éditorial permanent sur le cycle de production des contenus. Elles sont révélatrices de rapports de force et de stratégies qui nécessitent de voir ce qu'il y a au fond de la mécanique médiatique. C'est ce que propose de décrire la section suivante.

Procédures dans la construction des inscriptions

La principale fonction des soldats des médias est de créer des inscriptions regroupant des photographies, des vidéos, des enregistrements sonores, des textes, arrangées et filtrées par différentes techniques. Toutes ces inscriptions sont fabriquées à partir d'instruments aussi divers que des appareils photo, caméras, microphones, logiciels de traitement de texte, logiciels de montage photo et vidéo, etc. Elles sont en somme la « médiation de tout un appareillage » (Benjamin, 1963 : 289). C'est pourquoi les contenus dont nous avons été quotidiennement témoins lors de notre enquête ne peuvent se dissocier d'« un système d'intelligence distribuée » (Callon et al., 2001 : 97). Ce travail de fabrication et de stabilisation des inscriptions incluait nécessairement la coopération de corps disciplinés et d'instruments.

Derrière ces inscriptions se cachent ainsi des savoir-faire, des compétences, des habiletés et des matériaux. Quoique, à y regarder de plus près, ce professionnalisme est loin d'être si invisible que cela. À ce titre, un certain nombre de reportages photo produits par l'État islamique se sont concentrés sur la mise en scène des soldats des médias. Le soldat des médias, c'est d'abord quelqu'un qu'on reconnaît de loin : il porte un ensemble de signes, tels qu'un uniforme militaire, comme ses camarades au combat ; il manie non pas des armes, mais plusieurs équipements médiatiques sophistiqués. On le trouve en pleine action : il est sur le front, en train de filmer ou photographier les scènes de combats. Ainsi, au même titre que l'artillerie militaire, les équipements médiatiques n'échappent pas à des mises en scène. Ces

[63] Brochure « *Clarification Regarding the Media of Islamic State* »

images répondent à une même ambition : exposer la puissance du groupe. Elles témoignent de leur modernité, mais il y a plus. Elles sont aussi le symbole d'une appropriation de l'objet technique et de sa maîtrise.

Figure 5.3. Photo tirée d'un reportage photo officiel publié en 2017, montrant un homme muni d'un appareil photo numérique en train de photographier un bâtiment, qui sera sans doute la cible d'une attaque. La photo fait un plan sur l'écran de l'appareil, qui affiche un certain nombre d'options, montrant sa modernité.

Comme l'atteste la photo ci-dessus, les soldats des médias documentent. Ils permettent la première opération de « réduction d'échelle » (Callon et al., 2001). Le monde de l'État islamique sera soumis à des reproductions analogiques et numériques ; il sera simplifié et transposé dans des formats accessibles à une large audience. Ce complexe alliage corps-instrument ou humain-technique est ce qui permet le changement d'une matière dans une autre. C'est la première opération de traduction. Celle que Callon et ses collaborateurs (2001) décrivent comme « la réduction du grand monde (le macrocosme) au petit monde (le microcosme) du laboratoire » (p.83-84). Aucune ambiguïté ne doit résulter de cette simplification. À mi-chemin entre une recherche d'esthétisme et d'un réalisme pur, se dévoilent les images de la vie quotidienne sous le califat, ses victoires militaires, la mort des adversaires, la mise en scène des prisonniers, les drames humains, la camaraderie, les soldats sur le front, les pâturages, les montagnes, etc. Les soldats des médias fabriquent ainsi une diversité d'inscriptions qui doivent couvrir principalement quatre thématiques : les activités

militaires de l'État islamique, l'exercice de la charia[64], les services et activités de l'État islamique et la vie en général sous le califat.

Ces traductions successives suivront un ensemble d'instructions et de procédures. Dans les faits, aucun matériel brut ne peut être publié. Chaque contenu doit faire l'objet d'un cadrage au préalable. D'ailleurs, en visualisant les contenus de l'État islamique nous pouvions voir que rien n'était laissé au hasard. Si nous prenons le cas des contenus audiovisuels, le collectif manie habilement les codes visuels hollywoodiens et cinématographiques. Il va sans dire que cela inclut nécessairement la constitution d'un scénario. Nous avons ainsi pu lire dans le manuel destiné aux équipes de tournage :

> You should absolutely never go out for filming without a scenario. Everything has to be written in the scenario; starting from the message and idea that is intended to be delivered and ending with the angles of the shots. Some of the points that the mujahidin's scenario should contain: The message that meant to be delivered; A shape and description of the scenes (each scene should be carefully drawn) ; Angles of filming (the angles should be carefully drawn). [65]

Par ailleurs, comme cela était indiqué dans la brochure *General Guidance and Instructions*, l'innovation est quant à elle à proscrire : « we also advise the brothers to avoid innovation because it is mostly the main cause of mistakes ». En plus de cette prérogative, le *Média Central* a aussi mis en place un ensemble de règles à suivre pour les soldats des médias, dont nous avons pu retrouver les contours lors de nos observations quotidiennes. Dans les cas des reportages photo, pas moins de dix restrictions sont énumérées. En ce qui concerne les vidéos, les meilleures pratiques sont également indiquées :

Restrictions for photos reports	Restrictions of publishing a video release
1. The photo report should carry a clear idea which is the most important thing.	1. Unifying the design (fronts, introduction and conclusion)
2. Professional photography	2. The method used to compress the video release should be unified.
3. High definition photography	3. When there are big mistakes, the video should not be published. All mistakes should be corrected: the small and big ones.
4. Taking extra care of the first picture (the cover picture) with regards to the font and design	4. The brothers should appear in a very suitable
5. The number of pictures should not be less than 6	

[64] Selon le dictionnaire historique de l'islam la charia est l' « ensemble des prescriptions et des réglementations auxquelles le musulman doit se soumettre et qui portent à la fois sur la vie culturelle et sur les relations sociales » (Sourdel et Sourdel, 1996 :503).
[65] Brochure « *Media Mujahid on the subject of filming* »

pictures (including the cover picture), otherwise they'll count as individual pictures and would not be sufficient to deliver the idea behind a photo report. 6. All should try to stay away from repeating the same idea. 7. Unified design is a must (the officially approved template) (fronts and color). 8. Avoid repeating the same picture but from different angles unless it is very necessary to do so. 9. The numbering of a photo report should be based on the sequence of the report starting from the first day of the Hijri month. 10. The publisher should follow the unified form for tweets, which is: Wilayat #Aleppo, #Hama, #homs… etc. The title The link Pictures should be published alongside the tweet and should come directly under the tweet.	appearance, and they should be well spoken, and we will not accept anything less than that. 5. Filming should be done using more than one camera; any bad filming using one camera will be rejected.

Tableau 5.1. Critères et pratiques recommandées par l'État islamique pour faire des reportages photos et vidéo.

Ainsi, pourrait-on dire que les soldats des médias produisent un ensemble d'inscriptions pour qu'elles apparaissent à l'écran. Les contenus que nous visualisions au quotidien faisaient par conséquent l'objet d'une longue chaîne de mise au point, de méthodes et de techniques, ainsi que d'intermédiaires de toutes sortes. Ce que nous venons de soulever sur la réalisation des inscriptions nous permet de mieux saisir le fait qu'internet ajoute simplement une médiation à cette longue chaîne. En cela, cette prolifération de médiations rend improbable toute fétichisation du dispositif technique, c'est-à-dire que la propagande qui circule en ligne s'appuie sur un univers complexe d'intermédiaires et d'acteurs qui lui donnent toute sa validité.

En résumé, en parcourant la structure médiatique on s'aperçoit que la propagande de l'État islamique est très peu autonome. Elle tient en une série de contraintes, d'interdits et d'obligations. Cela s'explique entre autres parce que la construction des énoncés est collective et qu'elle dépend de différents niveaux de production et de validation. Certes, les documents ne fournissent qu'une indication et ne permettent pas d'attester comment ces règles étaient appliquées (si elles l'étaient) et comprises par les Bureaux des médias. De plus, ils ne nous disent rien sur l'effet de la coalition internationale sur l'organisation médiatique. Malgré la

perte de territoire et de cadres des médias, le groupe s'est montré résilient à produire de la nouvelle propagande (Milton, 2018 ; Winter, 2018). Certes, une baisse des contenus a pu être constatée[66], mais est-ce là une stratégie du groupe pour continuer à produire des contenus de qualité ou cela est-il révélateur d'une perte d'effectif ? À ce stade, plusieurs scénarios peuvent être envisagés, sans avoir de réponses concrètes sur l'état actuel de leur structure médiatique.

5.2.2. L'enrôlement des partisans

Pour diffuser ses inscriptions, l'État islamique aura besoin de consolider de nouvelles alliances, avec un réseau d'acteurs plus décentralisé. Pour que de nouveaux acteurs soient enrôlés, le collectif a mis en place une série de dispositifs d'intéressement passant par des communiqués, des images et des textes. Ces textes et visuels sont généralement conçus par des centres médiatiques pros État islamique ou encore par les partisans eux-mêmes. Intéresser de nouveaux alliés, c'est recourir à l'art de la persuasion et transmettre des mythes mobilisateurs à travers différentes techniques. Dans les mots de Callon et ses collaborateurs, intéresser c'est finalement « l'ensemble des actions destinées à produire de l'intérêt et à susciter l'adhésion d'acteurs influents » (2001 : 104). C'est donc par l'intéressement que le collectif composera un ensemble de forces pour obtenir un appareil de propagande efficace. Nous avons déjà vu précédemment la manière dont le collectif travaille à représenter l'utilisateur partisan de l'État islamique comme un être belliqueux. Toutefois, l'enrôlement des partisans se traduit également par d'autres moyens.

1° La valorisation du travail médiatique est devenue un élément central dans leur rhétorique. Le travail du collectif est de mettre en scène un internaute à part entière. Ce glissement est favorisé par la construction d'un nouvel utilisateur qui mélange langage militarisé et action médiatique : « chevalier des médias », « soldats des médias », « vétérans du jihad médiatique ». Les statuts d'utilisateur et d'internaute ne sont plus les variables principales qui le définissent ; mais sa vaillance, sa force, son combat. L'internaute devient un guerrier au même titre que ses frères qui combattent sur le front.

[66] Dans son étude longitudinale de la propagande de l'État islamique, Winter (2018) montre par exemple que l'infrastructure médiatique de l'organisation était environ deux fois moins productive au début de 2017 qu'à la mi-2015. L'auteur montre qu'à la fin de l'été 2015 l'organisation contenait 38 bureaux des médias et avait produit plus de 892 contenus uniques de propagande, alliant des longs métrages documentaires, des courts extraits des lignes de front, des reportages photo, des déclarations audio, des magazines, des livres et des pamphlets. En 2017, le groupuscule a produit 463 contenus, faisant chuter sa production de 30%. Outre une diminution des vidéos de haute qualité, la composition médiatique de l'État islamique était à peu près similaire en 2017 qu'en 2015.

2° L'important est de responsabiliser le partisan pour le faire prendre part au front médiatique et rendre effectives cette guerre et ses batailles :

> Les Soldats du califat ont entraîné les adeptes de la mécréance dans une guerre sanglante et éprouvante. Les affrontements féroces font rage dans chaque contrée et les *mujâhidîn*, arme à la main, affrontent sans répit, les ennemis d'Allah afin d'éradiquer l'idolâtrie. Quant à vous, ô partisan(e)s du califat, ô frères et sœurs en Allah, ne soyez pas dans l'attente des publications et communiqués ! Invoquez Allah sans qui les victoires ne sauraient être possibles. Publiez et partagez les informations, prenez le contrôle des réseaux sociaux et participez à la guerre médiatique. Qu'Allah bénisse les mains par lesquelles la vérité éclate jour après jour.[67]

Très clairement, ce type de communication montre que l'appareil du combat est élargi. Il couvrirait le territoire d'une nation, et dans un registre autre, celui des technologies de communication. Le combat doit être mené sur tous les fronts. Au sein des technologies numériques, cela doit concerner tout le monde ; homme-femme ; de n'importe quel âge ; partout à travers le monde. Point de système de recrutement, seulement un attachement à la cause. Aucune formation requise, des compétences élémentaires suffisent. En quelque sorte, une manière simple de participer au combat mené par l'État islamique. Cette masse d'utilisateurs enrôlés constitue sans doute la main-d'œuvre la meilleure marché : ils ne sont à charge de personne.

3° Parallèlement, le soldat des médias est représenté dans un nouveau style, celui du « jihadiste-hacker ». Les différences entre la culture *hacker* et le jihadisme sont suffisamment patentes pour qu'il soit superflu de les commenter en détail. Comme l'explique de manière claire et succincte Coleman « geeks and hackers build and configure technology at work and for fun, communicate and collaborate copiously with one another using these technologies, and, most significant, derive and express deep pleasure and forms of value by inhabiting technology » (2011 : 512). Le *hacker* est l'expression vivante de la symbiose entre l'homme et la machine (Levy, 2014). Il est le virtuose de la maîtrise de l'informatique. Certains militants de l'État islamique ont réinterprété les codes visuels des *hackers* tels que les pièces sombres éclairées par des écrans d'ordinateur, les rebelles *nerds* à capuche, les visages masqués ou invisibles. Certains visuels ont été jusqu'à reprendre le masque de Guy Fawkes, symbole même du groupe Anonymous (Coleman, 2016). Fait paradoxal était donné

[67] Communiqué non-officiel *« Ô Partisan du Califat »*, diffusé sur Telegram le 31 mai 2017.

qu'Anonymous combat fermement le groupe jihadiste, comme nous le verrons dans une autre section.

Le jihadisme puise une expérience tout à fait spécifique en s'inspirant de la culture *hacker* ; l'esprit anonyme, libre, solitaire et rebelle semble parler aux jihadistes. On est loin des symboles qui rappellent l'islam passé ou le jihadisme. Cette fois-ci, le jihadisme est numérique. Il est moderne. Il symbolise la maîtrise du système informatique. Comme le démontre la figure 5.6, on s'imagine dès lors un soldat des médias expérimenté qui opère dans le secret et travaille dans l'ombre pour combattre son ennemi. Il conjugue puissance, pouvoir et mystère. Cette appréciation libre des partisans cultive une description sans doute exagérée de leur statut en se présentant comme des super-héros du net. Si le propos n'est pas d'évaluer la juste nature de cette association au regard de l'islam, elle reflète toutefois quelque chose d'important chez les partisans : leur aspiration à se représenter comme des spécialistes de l'informatique. Ainsi, en mélangeant les genres, les concepteurs de ces visuels utilisent un symbolisme familier à la culture numérique pour réaliser un soldat des médias réinventé. Une figure sans doute séductrice pour les partisans immergés dans la culture informatique.

4° Il reste à convaincre que les partisans peuvent facilement devenir des soldats des médias ; que l'action peut être menée rapidement et sans grandes compétences techniques. Cela passe par des injonctions qui privilégient des actes simples comme le téléchargement et le partage des contenus officiels de l'État islamique. Un dispositif facilité par le web 2.0 en raison de son approche collaborative et de ses fonctionnalités de « partage ». Ces premières tentatives de lier concrètement le partisan au dispositif technique, misent ainsi sur des usages qui ont pour vocation d'amplifier la voix de l'État islamique. Ce n'est pas l'audace ou l'inventivité qui est demandée aux partisans, mais l'aisance, la rapidité et l'habileté à propager les contenus. Ils doivent agir en tant que relais des spécialistes des médias. Il faut qu'ils transportent « dans le grand monde » l'ensemble du matériel médiatique officiel produit par l'État islamique. Comme l'évoque une publication sur Telegram par un partisan pro État islamique :

> Why I call us media mujahids ?
>
> Many people you'll come across will make fun of you for calling yourself it but in reality you're !!

> The brothers of frontlines fight enemies of Allh swt with their weapons. Brothers in media department record, edit and upload it…
> Then comes our part if we won't be sharing the hard work they put into it all how would it be circulated ?
>
> By Allah you're part of the jihad. (Chaîne Telegram, 11 juillet 2017)

Malgré que les partisans saisissent le dispositif dans d'autres fonctionnements comme nous le verrons dans le chapitre suivant, nous pouvons d'ores et déjà établir que le collectif construit un « utilisateur fonctionnel », en ce qu'il remplit la fonction simple et efficace de relayer les contenus. L'ordonnance de la visibilité repose sur l'efficacité des partisans et de leur capacité à assurer le maintien du flux informationnel. Créer cet utilisateur fonctionnel implique un système d'action où les activités en ligne s'élargissent à l'automatisme. Ce faisant, les partisans sont réduits à des rouages machiniques ; quant à la mobilisation, elle devient plus automatisée. Cette phase de machinisation des corps ne fait pas l'objet de contestation. Au contraire, elle est valorisée au sein du collectif, puisque dépeinte comme permettant à la cause d'atteindre une large visibilité.

Figure 5.4. Image non-officielle valorisant l'action médiatique. Le partisan investi dans la cause médiatique sera comparé à un mujâhid.

Figure 5.5. Image non-officielle incitant les partisans à prolonger le combat dans les médias.

Figure 5.6. Image non-officielle comparant le soldat des médias à un hacker.

Figure 5.7. Visuel non-officiel incitant les partisans à participer à la guerre médiatique avec des actes simples et rapides.

Tableau 5.2. Exemples de visuels incitant à la guerre médiatique diffusés sur Telegram en 2017 et 2018.

5.2.3. Le *botnet*

Un troisième type d'acteur va maintenant concerner directement les machines. Au cours de notre enquête, nous avons régulièrement été confrontées à des *botnets* qui assuraient une série de fonctions : détection de virus en scannant les fichiers publiés sur Telegram, gestion des chaînes et groupes Telegram ou encore diffusion automatisée de contenus, pour n'en citer que quelques-unes. L'existence des *botnets* n'est pas en marge du réseau, mais pleinement intégrée au fonctionnement de la propagande de l'État islamique. Lorsque ces forces informatiques sont en action, le code et les personnes deviennent solidaires dans leur lutte, ils ne forment plus qu'un, ce qui permet au botnet de devenir en quelque sorte le porte-parole de la cause. Intéresser les *botnets*, c'est les fixer à du code. Une opération qui ne peut se dispenser de programmeurs. Cela nécessite donc une série de transactions entre humains et non-humains pour que progressivement, le botnet puisse incarner le rôle qui lui est attribué.

La présence non négligeable de *botnets* dans les processus politiques de l'État islamique témoigne d'une démocratisation sur le plan de leur conception et de l'ouverture de plusieurs plateformes à la perspective de les abriter. Sur Twitter, par exemple, il est permis sous certaines règles, de diffuser automatiquement des Tweets ou encore de proposer des réponses automatiques aux utilisateurs par Messages privés ou non. Grâce au fait que la plateforme fournit aux utilisateurs et aux développeurs un accès programmatique à la plateforme via leur API[68], il est maintenant à la portée d'un grand nombre de partisans avec une faible expertise en programmation de créer leur propre *botnet*. Cette expérience est similaire sur Telegram. Telegram décrit ses *bots* de la manière suivante : « Bots are simply Telegram accounts operated by software –not people- and they'll often have AI features. They can do anything – teach, play, search, broadcast, remind, connect, integrate with other services, or even pass commands to the Internet of things »[69].

Prenons pour exemple le *botnet* Khilafah Tube qui a été déployé sur Telegram aux alentours de décembre 2017. Khilafah Tube est la concrétisation d'une articulation entre le travail du

[68] De manière générale, Twitter explique que « les API permettent aux programmes informatiques de « se parler » entre eux pour demander et fournir des informations » (voir À propos des API Twitter : https://help.twitter.com/fr/rules-and-policies/twitter-api). En d'autres termes, c'est un moyen pour permettre à un logiciel d'offrir des services à d'autres applications. Avec les API disponibles, il sera dès lors possible de créer des logiciels qui s'intègrent à la plateforme. À la différence des individus qui accèdent à la plateforme via son site web ou via des logiciels clients, les *botnets* accèdent à ces sites par le biais d'une connexion de code à code, permise notamment par leur API (Dubbin, 2013).

[69] Voir Telegram Bot Platform : https://telegram.org/blog/bot-revolution.

code et d'une idéologie jihadiste. Toutefois, pour que cette concrétisation puisse avoir lieu, il a besoin de l'humain, pour reprendre l'expression de Simondon, comme « organisateur permanent » (1958 : 12). Cette dimension est régulièrement tue par les plateformes numériques, préférant présenter leur *botnet* comme autonome et intelligent. À propos des machines automatisées, Simondon explique que la tâche de l'humain ne se limite pas à surveiller la machine. Il est ce qui lui permet de fonctionner en lui attribuant des fonctionnalités. En cela, nous pouvons dire que Khilafah Tube fonctionne avec l'humain, car « ce qui réside dans les machines c'est de la réalité humaine, du geste humain fixé et cristallisé en structures qui fonctionnent » (Simondon, 1958 : 13). Toutefois, une fois que le *botnet* est programmé par son concepteur, « c'est la machine elle-même qui devient principale lectrice du code une fois que ce dernier y a été introduit » (Hayles, 2015 : 50). À la suite seulement de cette lecture, la machine affichera à l'écran des messages intelligibles pour l'homme.

D'entrée de jeux, nous sommes informés que Khilafah Tube est un *botnet*. Cela découle des caractéristiques techniques de Telegram qui oblige les *usernames* donnés aux *botnet*s de se terminer par *bot*. Ici, les *botnets* n'ont pas pour vocation de se fondre avec les êtres humains. Lors des interactions en ligne, une nette distinction doit pouvoir être effectuée entre les humains et les non-humains. À première vue, son concepteur s'est largement inspiré de YouTube pour créer le nom de son *botnet* ainsi que son logo. Quand on examine l'interface du *botnet*, on retrouve *grosso modo* les mêmes éléments graphiques que YouTube. Ce qui a changé, c'est une partie du nom et la couleur.

Pour former Khilafah Tube, *You* est remplacé par *Khilafah*. Ensuite, du rouge de YouTube, on passe au noir, rappelant l'étendard employé par les jihadistes de l'État islamique. Tout comme YouTube, le *botnet* est spécialisé dans le partage de vidéos, mais pas de la même façon. Le détournement sémantique et visuel de YouTube, n'augure aucunement que cela puisse représenter les valeurs et le fonctionnement de la plateforme. Alors que YouTube est une plateforme qui permet à tout internaute de publier et partager des vidéos pour faire entendre sa voix, le *botnet* Khilafah Tube agit de façon plus fermée. Face au choix délibéré de son ou ses concepteur(s), le *botnet* est dédié à diffuser les vidéos de l'État islamique. Cet agencement ordonne nécessairement un nouveau rôle au *botnet*, celui de participer à la représentation d'une idéologie politique parmi une masse d'autres représentants humains et non-humains.

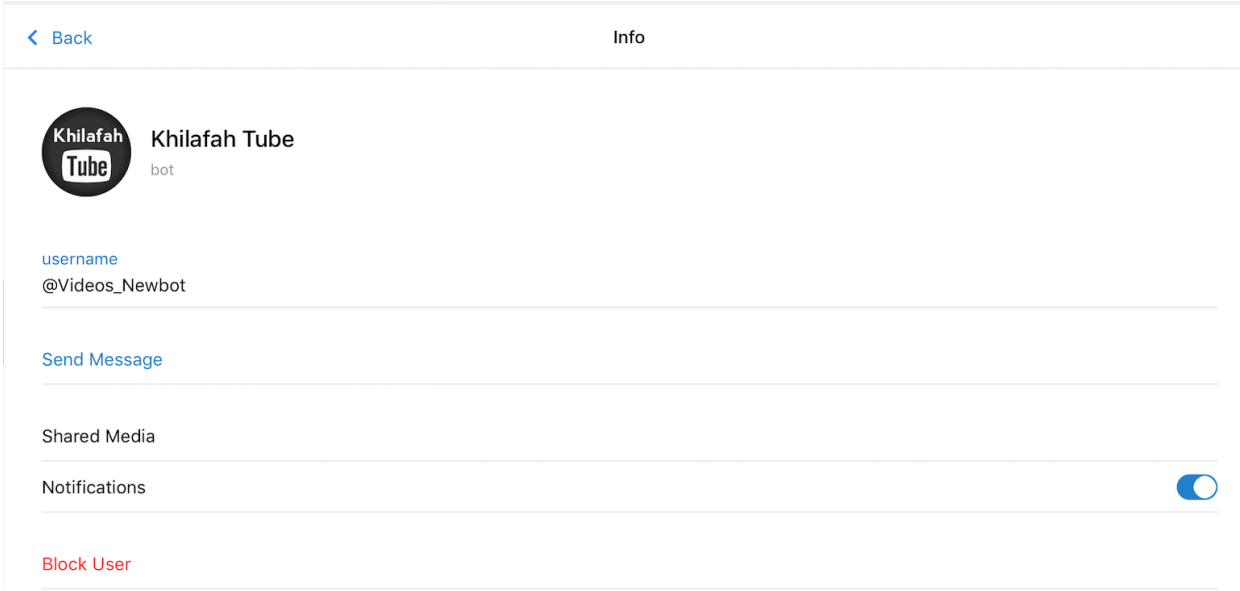

Figure 5.8. Fiche d'information du *botnet* Khilafah Tube, enregistrée le 6 décembre 2017.

Khilafah Tube, ne se contente pas de diffuser du contenu sur plusieurs groupes ou chaînes Telegram de manière coordonnée comme il était coutume de l'observer dans d'autres cas. Tout comme il ne se fonde pas dans la masse d'utilisateurs « réels », comme d'autres botnets pro État islamique. Au contraire, il allait nous offrir une expérience personnalisée, en nous permettant d'interagir directement avec lui. Il faut noter que sur Telegram, on n'interagit pas avec les *botnets* de la même façon qu'on le ferait avec des humains. L'humain doit adapter son langage, dans le cas où il voudrait entrer en communication avec le *botnet*. Il s'agit d'un langage plus technicisé et plus succinct. Cela découle du fait que communiquer avec un *botnet* poursuit toujours le même objectif : lui assigner une commande. Le sens de ces agents automatisés dépend donc intégralement des fonctionnalités qui lui ont été assignées par le concepteur, comme avec Khilafah Tube qui se contentait de diffuser des vidéos de l'État islamique.

La syntaxe utilisée doit obligatoirement être celle de « `/commande` », sans quoi la communication avec le botnet est impossible. Les règles en matière d'interaction sont strictes : une commande doit toujours commencer par le symbole « / » et ne peut jamais dépasser 32 caractères. Nous comprendrons très rapidement que nos interactions avec cet automate seront extrêmement rudimentaires : elles se limiteront à lui donner un ordre qui, s'il est donné dans les conditions requises, pourra être exécuté. Les *botnets* sur Telegram sont incapables d'initier une conversation avec les utilisateurs. De ce fait, un utilisateur doit soit les ajouter à un groupe, soit lui envoyer un message en premier. Nous sommes donc très loin

des scénarios de robots intelligents tels que par exemple l'agent conversationnel Tay qui avait été développé par Microsoft en mars 2016[70].

> <V.C> `/Start`
>
> <Khilafah Tube> Congratulations ! You subscribed to Vidéos
> Use `/off` to pause your subscription

À la suite de cette première interaction, nous avons reçu la dernière production vidéo du centre médiatique Al-Hayat. Deux jours plus tard, la commande `/videopress` a été activée par le *botnet*, diffusant pas moins de 82 archives de vidéos officielles de l'État islamique hébergé sur le site videopress.com. Notre interaction en est restée là, le *botnet* ayant été supprimé par la suite. Au même titre que les chaînes et les groupes Telegram, ces automates ne sont pas exempts des risques de suspensions s'ils ne respectent pas les conditions d'utilisation de la plateforme. Bien que Telegram limite les suspensions sur sa plateforme, ce n'est pas le cas pour les militants de l'État islamique. Comme la plateforme l'indique explicitement dans les FAQ : « While we do block terrorist (e.g. ISIS-related) bots and channels, we will not block anybody who peacefully expresses alternative opinions ».

Si la sophistication de Khilafah Tube reste limitée (par exemple en n'étant pas capable d'engager une conversation), cet automate s'est toutefois démarqué pour automatiser la propagande en diffusant instantanément et simultanément une grande quantité de vidéo officielles de l'État islamique. L'automatisation de la propagande ressort ici avec plus de netteté. On voit se dessiner des formes technicisées de la propagande où le code « exécute » la diffusion d'opinions politiques. Si le *botnet* est totalement indifférent au type d'action politique qu'il perpétue, il matérialise un type d'action politique ; celui d'un rapport productiviste au flux informationnel. Mais bien plus que ça, il permet de perpétuer l'imaginaire politique auquel il renvoie. Ainsi, il n'est pas seulement une machine automatisée, mais aussi une machine symbolique.

[70] Tay est une intelligence artificielle capable d'interagir avec les internautes sur des réseaux sociaux et des applications de messagerie. Microsoft a du suspendre Tay au bout de quelques heures, à la suite qu'elle ait tenu des propos racistes et misogynies. Microsoft avait alors indiqué qu'un effort coordonné de quelques utilisateurs avait abusé des capacités de Tay pour qu'elle réponde de manière inappropriée. Pour plus d'informations voir : https://www.lemonde.fr/pixels/article/2016/03/24/a-peine-lancee-une-intelligence-artificielle-de-microsoft-derape-sur-twitter_4889661_4408996.html

5.2.4. Les spécialistes en cybersécurité

Une des préoccupations quotidiennes du collectif est d'assurer leur sécurité opérationnelle. La sécurité opérationnelle ou Opsec, peut se définir comme « l'art d'assurer la protection des interactions humaines et numériques au sein d'un groupe » (Coleman, 2016 : 275). Pour assurer la sécurité opérationnelle et sensibiliser les utilisateurs à ces questions, des partisans de l'État islamique ont élaboré un vaste réseau de chaînes Telegram spécialisées dans les questions de cybersécurité. Ces acteurs, anonymes et insaisissables, incarnent la fonction même de porte-parole des défaillances techniques. Ces spécialistes en cybersécurité se voient confrontés à la tâche d'exposer le dispositif technique dans ses faiblesses. Ils mettent le doute face à une sécurité jugée peu fiable. Ces chaînes sont extrêmement diversifiées. On voyait se développer des chaînes qui se focalisaient sur un type seulement de logiciel et de vulnérabilités et d'autres qui traitaient de plusieurs thématiques de cybersécurité à la fois.

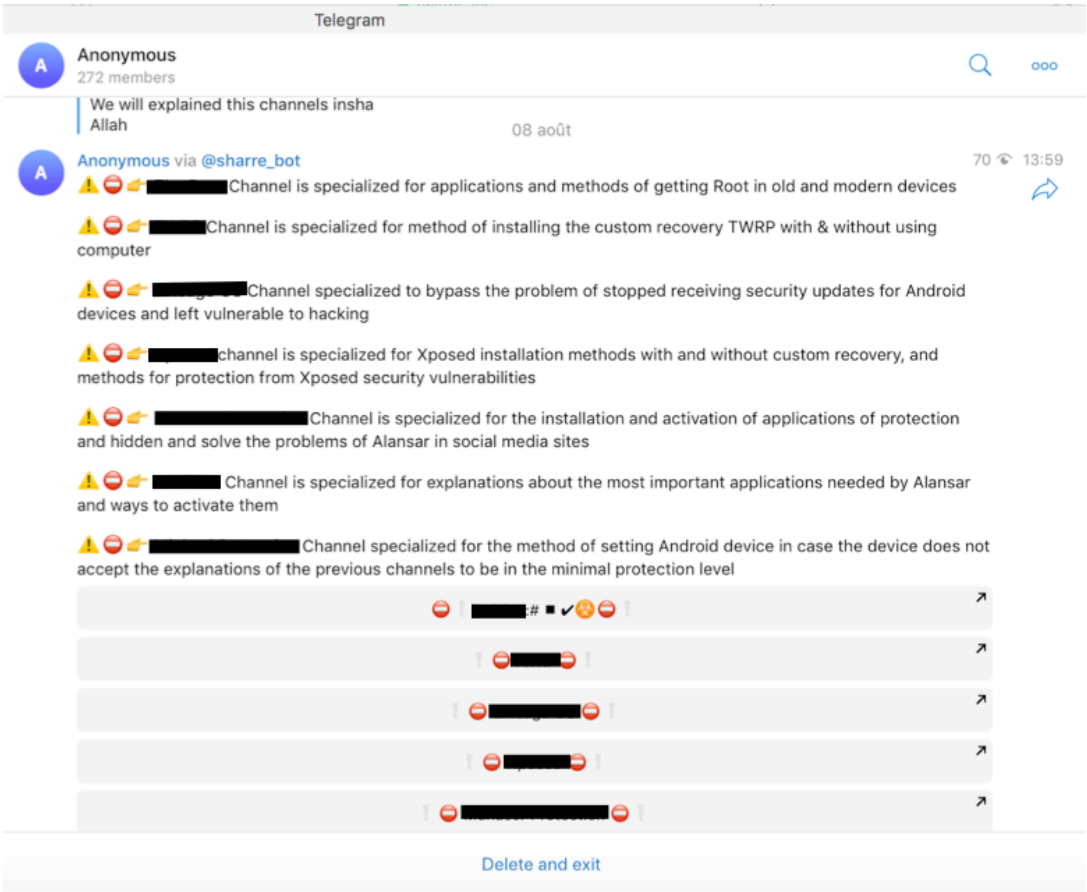

Figure 5.9. Exemple de publicisation de 7 chaînes techniques pro État islamique. Capture d'écran enregistrée le 9 août 2018.

Les stratégies de représentations de ces chaînes diffèrent des autres chaînes partisanes ou relais de l'État islamique. Le but cette fois-ci est d'invisibiliser leur appartenance au collectif.

Aucun étendard, aucune photo de combattants, aucun communiqué de l'État islamique n'apparaît sur ces chaînes. Les photos de profil sont celles d'androïde, de logiciels ou de manière plus officielle, le logo de leur fondation. Les noms des chaînes renvoient au collectif de cybersécurité directement ou à des logiciels. Pour perdurer dans le temps, elle emploie le ton le plus neutre possible. Par exemple, l'une des chaînes en cybersécurité les plus populaires, totalisant à elle seule plusieurs milliers d'abonnés et disponible en plusieurs langues, se décrit comme « une fondation indépendante qui vise à sensibiliser les musulmans à la sécurité en français ». Avec ces chaînes spécialisées, le collectif signale qu'il connaît et maîtrise la technologie, et qu'il est capable de mettre en place un système de défense pour se prémunir des menaces en ligne.

Le rôle de pédagogue

Toutes ces chaînes ont la même vocation : informer les utilisateurs des différentes menaces numériques auxquelles le collectif est exposé et les précautions à prendre. Ainsi, en plus de leur rôle de porte-parole des failles de sécurité, ces acteurs endossent celui de pédagogue. Il vise primitivement à poser les bases des précautions à prendre en matière de cybersécurité. Ils permettent la mise en œuvre de l'action de précaution. Ce rôle de pédagogue se déploie de trois manières : la création de guides, la sensibilisation aux enjeux de cybersécurité et enfin l'établissement d'une veille sur les dernières nouvelles en matière de sécurité informatique.

L'expertise est transmise au travers de tutoriels clairs et succincts qui sont directement publiés sur la chaîne ou alors prennent la forme de court guide en format PDF (pouvant aller de moins de dix pages à une soixantaine de pages) à télécharger. Ces tutoriels sont consacrés aux solutions techniques à mettre en place pour protéger les communications en ligne des utilisateurs. Prenons par exemple une chaîne qui se dit spécialisée dans la sécurité informatique à laquelle nous avons eu accès en août 2018. La chaîne commence avec le message d'introduction suivant :

> Le Centre Médiatique An-Nûr a le plaisir de vous présenter la réouverture de sa section sécurité informatique. Elle traitera de l'actualité en termes de sécurité et proposera des tutoriels PDF et animations.

Sur la chaîne, nous avons téléchargé pas moins de neuf tutoriels informatiques, dont les suivants :

1. Crypter son disque dur
2. Anonymisation via TOR et VPN
3. Installation d'Orbot et Orweb sur un Smartphone Android
4. Changement de l'adresse MAC pour Windows et MAC
5. Crypter et décrypter vos messages avec PGP
6. Vérifier l'authenticité de vos applications
7. Rooter votre Smartphone Android
8. Installation d'un VPN sur Android
9. Installation de TOR sur les différents systèmes d'exploitation

Généralement, ces derniers suivent tous la même structure. Ils commencent par définir le nouveau logiciel à télécharger et son utilité. Ensuite, des explications sont données étape par étape pour l'installation et le paramétrage de l'application. Pour que cela soit le plus accessible possible, les instructions sont formulées au moyen de courtes phrases et de captures d'écran. Ce format de tutoriel est similaire à ceux conçus par d'autres fondations de cybersécurité pro État islamique. Ces guides ont pour mission de proposer des solutions extrêmement techniques pour assurer la sécurité du collectif en ligne. On voit ainsi se dessiner les grandes lignes d'un système de précaution dont l'opérationnalisation dépend d'un ensemble de non-humains programmés par des humains qui limiteront d'éventuels dommages.

Pour sensibiliser davantage le collectif aux risques de cybersécurité, ces chaînes proposent aux partisans une série d'expériences ludiques. Notamment, plusieurs contenus prennent la forme de « *question/réponse* » ou de « *le saviez-vous ?* ». Il s'agit dans ce cas de traiter diverses thématiques de cybersécurité de manière concise et accessible pour des non-initiés. Cela représente inévitablement pour tout novice un moyen simple et accessible de comprendre une série d'enjeux en matière de risques informatiques.

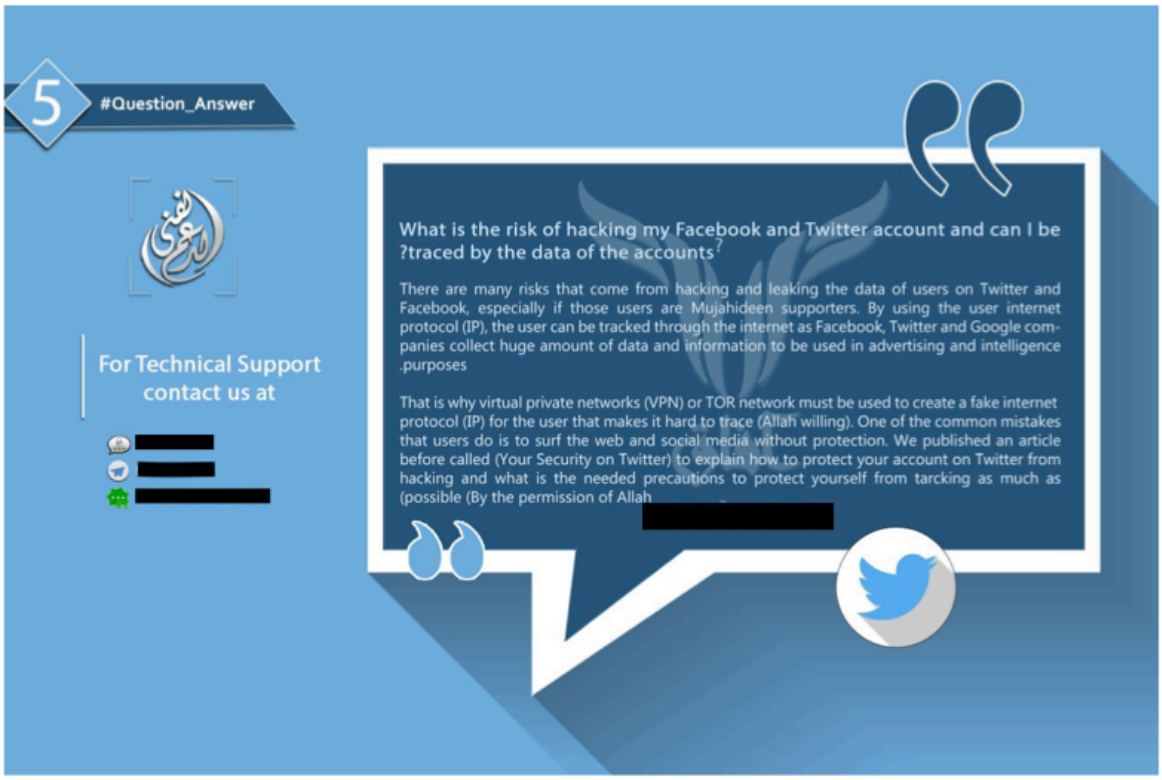

Figure 5.10. Exemple de question-réponse sur la thématique du piratage de compte Facebook et Twitter, publié par la fondation technique pro État islamique. Ce visuel a été diffusé en décembre 2018 sur une chaîne Telegram dédiée aux questions de cybersécurité.

Par ailleurs, face à un environnement changeant en matière de risques et de dangers, certaines fondations effectuent un travail de veille. Il s'agissait de publier chaque semaine en plusieurs langues un bulletin concernant les nouvelles les plus importantes en matière de cybersécurité. L'ensemble de ces informations est collecté à partir d'articles de presse et de sites web spécialisés sur les questions de cybersécurité. Failles et risques des logiciels, collectes de données de la part des gouvernements et entreprises privées, *hacking*, voici toute une série de thématiques qui sont abordées et permettent d'attester que la visibilité de l'État islamique se construit dans un environnement hautement risqué.

La surveillance à différents niveaux

Si les tactiques quotidiennes du collectif s'inscrivent dans une architecture plus participative, le collectif a bien conscience qu'elles s'exercent dans un environnement où les questions de surveillance constituent un enjeu crucial. Le collectif aime rappeler que les plateformes numériques basées aux États-Unis entretiennent des liens étroits avec la National Security Agency (NSA), comme l'atteste ce message d'introduction d'une chaîne Telegram spécialisée en cybersécurité :

> In this channel we will provide a detailed explanation of computer protection and hidden in the net
>
> And since most computer users are using the Windows system will be an explanation of this system.
>
> But we must first note that Microsoft is a spy company that collaborates with the US National Security Agency and violates the privacy of users, follows their steps on the computer and gathers all their data. Therefore, brothers should use alternatives systems to Microsoft products as we are looking for a complete Hidden in the net because the US National Security Agency and the crusader alliance considers us a treasure of valuable information that helps them target the Mujahideen and spy on them so you are responsible for your electronic security and responsible for the security of your brother Mujahid. (Chaîne Telegram, 29 mai 2017)

En même temps qu'assurer la visibilité du collectif, voici ironiquement les mesures qu'il fallait prendre : se rendre invisible sur internet. La surveillance peut compromettre l'identification de partisan et l'élaboration de plan militaire ou d'attaques terroristes, ce qui est extrêmement préjudiciable pour le groupe. C'est dans ce contexte que les chaînes spécialisées en cybersécurité multiplient les mises en garde. Comme ces collectifs le rappellent régulièrement, la surveillance se retrouve sur les réseaux sociaux, les navigateurs web, Adresse IP, MAC, DNS, cookies, téléphone mobile, métadonnées relatives aux images, microphones et caméras sur appareils mobiles, etc. Les risques de traçabilité proviennent à la fois des compagnies privées, des gouvernements, de logiciels malveillants et de *hackers*.

En plus d'aviser les partisans des dangers généraux sur le web, certaines de ces fondations avaient un rôle plus actif en créant des alertes lorsqu'un risque imminent était perceptible. Dans l'alerte ci-dessus, l'utilisateur suspect a diffusé sur des groupes et chaînes Telegram un site web qui permet de traquer « all the kuffar and spies ». Le site al21truth consiste à présenter « a list of trusted brothers and deceivers to help know who can be trusted and who cannot trust. Disbelievers are everywhere ». En somme, quelque chose qui peut susciter de l'intérêt dans un climat où tout le monde est suspect et où les jihadistes se lancent dans d'inlassables traques à espion. Si déjà quelques utilisateurs exprimaient leur doute quant à la validité de ce dispositif, ces doutes ont été confirmés par l'une des chaînes spécialisées en cybersécurité.

Figure 5.11. Mise en garde opérée par une fondation technique pro État islamique publiée sur Telegram en juillet 2018.

Finalement, chaque couche du dispositif technique (logiciel, hardware et contenu) qui permet la visibilité du collectif les expose à des risques de traçabilité. Toutefois, à ces risques identifiés aux nouvelles technologies, le web offre également de nombreuses alternatives et possibilités pour améliorer la sécurité informatique. Le collectif a ainsi une panoplie d'autres objets techniques pour agir de façon préventive et prendre des précautions. Comme le rappellent Callon et ses collaborateurs (2011), le principe de précaution encourage l'action, il ne l'aliène pas. Il exige de mettre en place un système de protection. On apprenait par exemple comment installer Tails, un VPN ou un pare-feu ; comment changer d'adresse IP ; comment se connecter au réseau TOR ; comment crypter ses appareils et son disque dur ; etc.

Certes si le collectif reconnaît l'existence de dangers au sein de l'espace où ils promeuvent leur visibilité, rien n'est dit sur le fait que les partisans s'empareront de ces alternatives. Ces savoir-faire peuvent effectivement représenter un coût cognitif supplémentaire (Boullier, 2012). Il ne suffit plus simplement de naviguer, de publier, de créer du contenu, il faut aussi assurer sa propre sécurité en ligne. Cela demande de mettre en place des alternatives qui nécessitent d'installer et de paramétrer des logiciels parfois très complexes. Par exemple dans

les 137 jugements d'individus condamnés en France dans des affaires de jihadisme analysés par Hecker (2018), une grande hétérogénéité en matière de sécurité informatique a pu être observée. Si certains prévenus n'avaient pris aucune précaution pour protéger leurs échanges téléphoniques ou numériques, des précautions importantes avaient pu être prises par d'autres afin de laisser le moins de traces disponibles sur internet. Généralement, les techniques utilisées référaient aux recommandations observées : utilisation d'application et de logiciel cryptés ; utilisation de logiciels masquant l'adresse IP ou encore la création de boîtes de messagerie électronique cryptées.

5.3. Réguler les habiletés techniques

Être visible en ligne cristallise pour le groupe un mode de vie avec des règles et des normes communes. Un ensemble de contraintes, d'interdits et d'obligations viennent réguler les habiletés techniques des partisans. L'anatomie de cette régulation est d'origine différente et de localisation éparse, mais l'ensemble de ces règles a pour finalité de se recouper, de se répéter, de prendre appui les unes sur les autres. Ces préceptes réglementaires sont diffusés par des sources officielles de l'État islamique ou des centres médiatiques non-officiels, sous forme de textes ou d'infographies. Ils peuvent également prendre la forme d'avertissement dans le cas de menaces perceptibles, comme une sorte de rappel à l'ordre.

Ces préceptes réglementaires ne font aucunement objet d'un débat ou d'une discussion ; ils sont acceptés tacitement. Tout comme aucune sanction directe ne sera exercée sur le partisan, elles ont plutôt pour fonction d'engager sa responsabilité. Il s'agit en quelque sorte d'une éthique de l'action, plus que d'un pouvoir disciplinaire, afin que l'usage individualisé n'entrave pas l'action collective. Ces règles s'adressent indissociablement à tous les « *partisans du califat* ». Il s'agit d'assurer une prise sur leur maniement du dispositif technique. Auquel cas, certaines conditions doivent être réunies pour que le déroulement de l'action puisse s'exercer efficacement. L'objet du contrôle ne concerne pas tant le résultat final, que le processus par lequel l'action doit se dérouler. Elle décrit un mode d'investissement avec la technologie, une façon de se comporter. Il s'agit de privilégier la précaution, d'assurer une cohérence dans la pratique, ainsi que d'être solidaire dans son fonctionnement. Ce qui importe réellement c'est l'efficacité du flux informationnel et leur

puissance de propagation. Cet objectif d'efficacité se décline sous différentes règles essentielles au bon fonctionnement du maniement du dispositif technique[71] :

1° *Ne pas rechercher la gloire*. Les règles d'utilisation des réseaux sociaux de l'État islamique sont incompatibles avec les notions de prestige personnel et de célébrité. Au sein de l'État islamique, il est proscrit aux partisans de rechercher la gloire sur les médias sociaux. L'objectif à poursuivre est le « soutien des moudjahidines » et non pas le « succès personnel » ou encore la recherche d'un « grand nombre d'abonnés ». Cette règle exige du partisan qu'il s'allie à la cause et se détourne de tout objectif individualiste : seul compte le travail au sein du collectif. Par ailleurs, on ne se préoccupe aucunement du résultat des actions en ligne, qui est du ressort d'Allah. Nous pouvions ainsi lire sur l'infographie traduite du journal An-Naba : « Allah ne nous a pas chargé sur résultat, cela est certes entre les mains de celui qui connaît toutes choses, mais œuvrez et par votre sabab (cause), par la grâce d'Allah le majestueux, vous obtiendrez une abondance de résultat ». On comprend que le concept de l'action en ligne est extrêmement collectif. Il renforce la tendance à la révélation de la cause, et non pas de l'individu. Le partisan est d'abord un producteur et un relais des flux informationnels. Ils ne viennent pas pour se faire-voir, ni pour être populaires, mais bien pour propager la cause du groupe. Les pratiques doivent dès lors s'enligner vers des stratégies qui préconisent l'appartenance au groupe et la circulation du flux informationnel pro État islamique. Si dans ce contexte, on peut difficilement devenir célèbre, cela n'a toutefois pas empêché la formation de ce que Gerbaudo (2012) appelle des « 'soft' forms of leadership ». À ce titre, au sein de la jihadosphère, certains utilisateurs sont devenus de véritables références. Leurs chaînes Telegram peuvent cumuler plusieurs centaines de membres très rapidement, contrairement à d'autres qui se soldent par un faible succès. Ces utilisateurs sont habiles pour susciter l'intérêt des spectateurs, en publiant à la fois les derniers contenus de l'État islamique, des nouvelles géopolitiques, des informations provenant des médias *mainstream*, des contenus sur leurs adversaires et des contenus religieux.

2° *Bannir la paresse.* L'action est présentée comme la seule expérience possible pour rependre la « vérité ». Le partisan ne peut se réduire au statut de spectateur : il doit agir, déclencher des processus sans précédent. La paresse est stigmatisée, critiquée et méprisée au

[71] La plupart de ces injonctions ont été résumées dans une infographie officielle intitulée « *Partisans du califat dans les médias* » produite par le journal An-Naba en septembre 2018. Cette infographie, publiée en plusieurs langues, a été largement diffusée par les partisans de l'État islamique.

sein du collectif : « résistez à la paresse et l'ennui, si cela arrive, le remède est la satisfaction et l'effort constant ». Ce qui est attendu du partisan c'est qu'il n'arrête jamais de performer. Dans cet aspect de l'action, le partisan doit continuellement « développer des talents et des compétences ». L'habileté et l'aisance à développer de nouvelles compétences sont des ingrédients essentiels pour la réussite de l'action : « Diversifiez vos activités médiatiques, développez vos talents, continuez à progresser sans jamais vous arrêter ». À cela, il incombe à l'utilisateur de s'évaluer et d'apprendre de ses erreurs. L'expérience et l'expertise sont ainsi d'autres qualités primordiales promues par le collectif : le partisan aura mémorisé un ensemble de configurations médiatiques qu'il a au fur et à mesure corrigé ou répliqué selon les succès. Il est dès lors attendu du partisan qu'il ajuste ses talents et compétences, en puisant dans cette « réserve » d'usages, d'habitudes ou de réflexes.

3° *Vérifier l'information propagée*. Au cours de leur activité en ligne, certains moments seront parsemés d'épreuves, testant continuellement l'habilité du collectif à résister aux différentes menaces. Parmi les principales, on retrouve celles qui visent à miner la confiance au sein du collectif en propageant des fausses informations. La circulation de fausses informations par les opposants est un vieil héritage. Par exemple, dénommées comme des « mesures actives » par le KGB, les études sur la propagande à l'époque de la Guerre froide ont démontré trois types de répertoires propagandistes utilisés par les Soviétiques (Benkler et al., 2018). La propagande « blanche » qui se réfère à un organe officiel et dont les informations, plus ou moins justes, visent à promouvoir le parti. La propagande « noire » consiste à diffuser des informations mensongères par des sources fausses et hostiles. La propagande « grise » est quant à elle un entre-deux. Les adversaires de l'État islamique se sont régulièrement adonnés à faire circuler de fausses informations.

Il s'agit pour la plupart de ces tentatives de diffuser des faux communiqués, de faux exemplaires de leur matériel médiatique et de fausses chaînes Telegram ou compte Twitter. Ces actions stratégiques peuvent différer. Par exemple, les fausses déclarations d'Amaq ou celles attribuées à l'État islamique se doivent d'être le plus crédibles possible afin qu'elles puissent être relayées par les partisans de l'État islamique. Ainsi, il s'agit de changer quelques éléments opérationnels pour que le doute entre fiction et fait soit constant au sein des partisans. Il s'agit là d'une nouvelle traduction plus subtile que le simple fait de contredire l'information par des mensonges ou alors d'introduire du contenu satirique ou pornographique comme cela a été le cas. L'objectif de ces campagnes successives,

généralement de sources anonymes, est de semer confusion et doute chez les participants de l'État islamique, et à terme de saper leur confiance auprès des organes de propagande de l'État islamique. Les partisans de l'État islamique ont ainsi commencé à multiplier les mises en garde face aux tentatives d'usurpation et de faux contenus dont ils étaient victimes :

> There is currently a group of fake (Amaq Agency) channels that are broadcasting false information, and this directly affects the ansar channels, be sure to identify the channels and exit them, do not be part of their falsehood. Fake Account : #AMQ_Support. (Groupe Telegram, 18 novembre 2017)

Parallèlement, pour parer à ces flux nuisibles, le collectif engage la responsabilité du partisan dans son devoir de vérifier l'information qu'il relaie. Pour répondre aux exigences voulues par les instances officielles de l'État islamique, le partisan ne devra s'en remettre qu'au média officiel. Nous pouvions lire sur l'infographie d'An-Naba : « Vérifiez avant de rapporter, conformez-vous au média officiel du califat, car il est le plus fiable et le plus véridique ». Le devoir de vigilance doit être de même pour le téléchargement de contenus officiels de l'État islamique, qui pouvait tant contenir de fausses informations qu'être infecté par des virus et malwares. Ainsi, le collectif a stipulé à maintes reprises dans des infographies diffusées à cet effet : « it is always advised to refer to official Islamic State media sources when downloading material. Downloading from elsewhere is dangerous and such content may include fake or infected material » (voir figure 5.11.).

4° *Maintenir la sécurité en ligne*. Nous avons déjà largement souligné comment la cybersécurité fait l'objet d'une vaste préoccupation au sein de l'État islamique. Il s'agit de pouvoir se prémunir de tous les comportements nuisibles (piratage de comptes, malware, *spam*) et de prendre des précautions pour éviter toutes fuites d'informations et de renseignements personnels vers l'ennemi. Dès lors, du fait que l'incertitude et les risques en matière de cybersécurité sont grands, la précaution en matière de sécurité de l'information devient une obligation individuelle. Comme l'indique un paragraphe de l'infographie du journal An-Naba :

> Maintenez votre sécurité et soyez prudent, ne négligez pas cela, car le maintien de sécurité est considéré comme une obéissance essentielle. Employez vos efforts dans votre sécurité, mais ne permettez pas à cela de se tenir tel un obstacle entre vous et votre soutien, car la sécurité est destinée au travail et non à la stagnation.

Ainsi, une grande partie du travail du partisan consiste à sécuriser sa relation avec le dispositif technique. Cet impératif ne sert pas seulement une cause purement individuelle, mais sert le groupe tout en entier[72]. En cela, il est régulièrement rappelé aux partisans qu'en assurant leur sécurité, ils assurent aussi celle de ses frères. Les partisans qui délaissent leur sécurité risquent quant à eux de vives critiques. Dans ce climat où leur visibilité les expose à plus de vulnérabilités, utiliser le dispositif technique requiert un ensemble de compétences qui visent à stabiliser leur environnement en se protégeant d'une série de menaces.

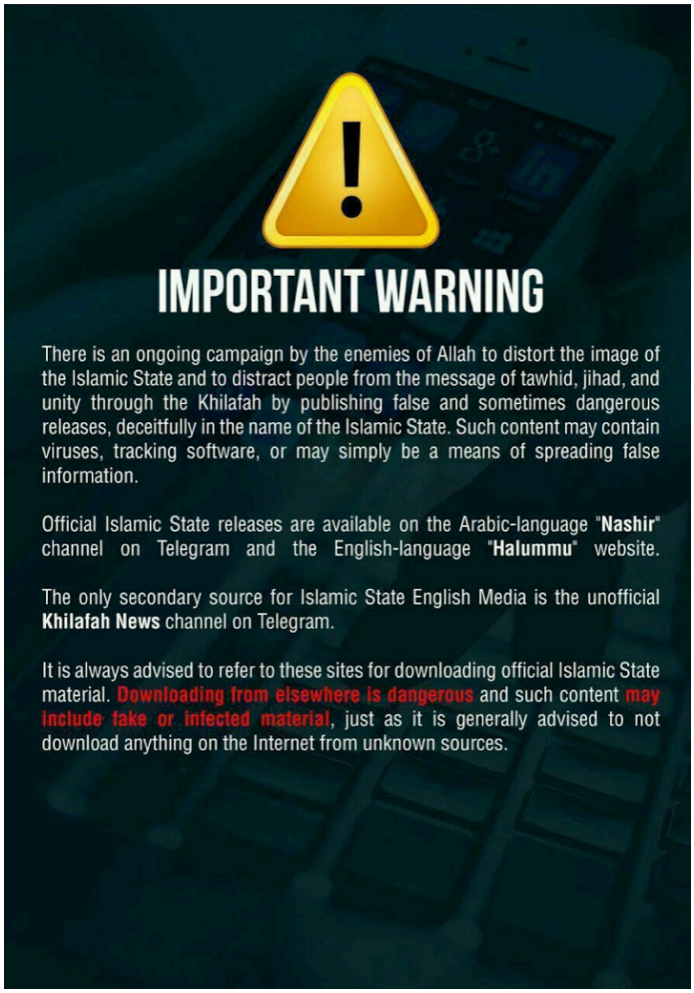

Figure 5.12. Exemple d'un avertissement publié sur Telegram en 2017 par des militants de l'État islamique. Ce type d'avertissement était régulièrement distribué au sein de la sphère jihadiste.

[72] Outre le fait que l'utilisateur peut exposer inutilement d'autres des partisans aux services de renseignements, cette « obligation individuelle » trouve aussi sa légitimité dans le fait qu'elle permettrait de protéger le collectif de mécanismes de surveillance des réseaux sociaux toujours plus ubiquitaires. Par exemple les plateformes ne collectent pas toujours uniquement les données personnelles de l'utilisateur, mais aussi de son réseau d'amis, selon les applications utilisées. Vaidhyanathan (2018) explique que : « if you have been active on Facebook since before 2014 and you interacted with games or applications like Farmville, Mafia War, or Words with Friends, then Facebook exported not only a rich collection of your profile and activities on Facebook but also those of you Friends » (p. 57). Un mécanisme qui s'est renouvelé avec le scandale de Cambridge Analytica en 2018.

5.4. Théâtraliser les compétences techniques

32 140 reportages photo. 4 540 textes. 2 880 vidéos. 1 670 audios. En tout, ce ne sont pas moins de 41 230 contenus médiatiques qui ont été produits entre 2014 et 2017. C'est du moins ce que révèle une infographie produite par un centre médiatique pro État islamique[73]. Peu importe que ces chiffres soient véridiques ou non, on comprend que le collectif veut attester sa puissance médiatique. Les chiffres sont ici un outil de propagande qui cherche à décrire la manière dont ils produisent et reproduisent leur puissance médiatique. C'est ainsi qu'au cours de notre enquête, nous avons rencontré à quelques reprises une trame de supports infographiques non-officiels comprenant des statistiques et des données qui avaient pour objectif spécifique de quantifier l'activité du collectif. Les statistiques pouvaient être trimestrielles ou alors faire le bilan sur plusieurs années. Le but était de documenter statistiquement le travail des médias officiels et des partisans.

Ce type de procédé est comparable aux infographies qui contiennent les statistiques d'opérations militaires de l'État islamique. Si les comptes rendus des opérations médiatiques sont nettement plus rares que ceux des opérations militaires, lorsqu'ils sont produits, ils font l'objet d'un grand retentissement chez les partisans. Ces derniers ne s'attardent pas seulement à les relayer au sein de la sphère jihadiste, mais les propagent au sein des cercles ennemis. Une manière de faire, était d'utiliser des *hashtags* tendances ou non sur Twitter, par exemple lorsqu'un centre médiatique pro État islamique a fait le bilan de ses deux ans d'activité, ce dernier avait publié plusieurs *tweets* à ce sujet dont : Statistical work of Islamic supporters https://t.co/----- #OTDirecto19N #BreakingNews (Twitter, 20 novembre 2017).

De façon générale, ces statistiques ont un rôle résolument stratégique : elles communiquent sur la réalité des opérations médiatiques et sur les compétences techniques du collectif. Il est aisé à partir des statistiques de dresser le constat sans équivoque d'un succès médiatique. Ainsi, il est en quelque sorte la théâtralisation des « habiletés techniques » (Dodier, 1993). Toutefois, de cette dramaturgie, sont exclus les intermédiaires techniques qui permettent le succès de telles opérations. Pour Dodier, cela revient à « imputer les résultats de l'activité technique à des capacités détenues en propre par l'utilisateur » (Dodier, 1993 : 130). Le prestige des actions repose alors entièrement sur les qualités du collectif qui « possède donc des aptitudes intériorisées de maniement de la machine » (Dodier, 1993 : 130).

[73] Infographie non-officielle « *Three years on the Islamic State* », juin 2017

Pour faire valoir ses habiletés, le collectif doit également confronter son succès à l'échec de la lutte antiterroriste. La mise en valeur de leur virtuosité consiste à donner suffisamment d'informations aux spectateurs pour qu'ils repèrent les menaces à travers lesquelles le collectif doit exercer son action. Il n'est pas question pour le collectif de dire comment il manie le dispositif technique, gardant une part de secret, mais de rendre compte de ses résultats dans un contexte où il fait constamment l'objet de suspensions. Le but : montrer les capacités de résilience du collectif. Ces procédés narratifs se traduisent de plusieurs manières :

1° Le collectif cherche à affirmer sa virtuosité à partir de stratégies calculant le nombre de contenus publiés chaque jour en ligne et le nombre de nouveaux comptes qui seront créés par les partisans de l'État islamique, malgré les suspensions répétées dont ils font l'objet. Si totaliser le nombre de nouveaux comptes et de publications en ligne est tout bonnement impossible, et semble se livrer à un exercice plutôt hasardeux, le grossissement de ces chiffres est une manière pour le collectif de montrer que leur présence ne s'effondre pas à la suite de la lutte antiterroriste en ligne. Au contraire, ils démontrent qu'ils sont dans une optique de conquête et que leur présence est inévitable. Ils perpétuent l'idée qu'ils disposent de toutes les compétences techniques pour réapparaître en ligne et afficher leur propagande.

2° Inévitablement, ils visent à ridiculiser l'ennemi. Tandis que d'un côté le collectif recense ses opérations médiatiques, d'un autre il dénombre les opérations antiterroristes en ligne et le coût de ce type d'actions : « 40 services de renseignements combattent l'État islamique en ligne sur différentes plateformes » ; « plus de 4 000 comptes sur les réseaux sociaux et sites web ont été supprimés » ; « plus de 1 000 000 dollars ont été dépensés dans la guerre médiatique »[74], pouvait-on lire sur une infographie pro État islamique. Le fait que le collectif expose ses réussites et les échecs de ses adversaires répond à un principe élémentaire de propagande, celui d'indiquer que les pertes de l'ennemi sont plus importantes que les leurs (Morelli, 2001). Ainsi, le collectif montre qu'il garde la main sur le dispositif technique malgré les puissants efforts déployés par les plateformes numériques et les gouvernements. Mieux, il veut démontrer que l'adversaire gaspille inutilement ses ressources. Et quoi de plus

[74] Infographie non-officielle « *Failure of the Media War on the Islamic State*», mai 2017

outrageant pour l'adversaire que d'être vaincu par un groupe ne disposant pas d'autant moyens financiers et techniques ?

> Et l'État Islamique et ses partisans continuent de conquérir et de se déployer sur le front médiatique diffusant des milliers de parutions par le biais de milliers de comptes dans des dizaines de langues chaque jour sur tous les réseaux sociaux sans avoir dépensé ce que les mécréants ont dépensé, sans avoir les capacités technologiques qu'ils possèdent et tout cela n'est que par la grâce d'Allah. Donc, ô partisan continue de plonger l'effroi dans le cœur des mécréants par la terreur des médias et de supporter ta communauté et ta religion[75].

3° Pour attester de sa puissance sur le front médiatique, le collectif fait également un usage habile de citations et de dépêches qui rendent compte des failles et des faiblesses de la lutte antiterroriste en ligne : « On a strategic level, the organization is winning the war in social media websites, its online platforms have become after each new assault a familiar place to go to for anti-terror experts where they search for statements from Amaq news agency website, the mouthpiece of the organization - Foreign Affairs ». Il s'agit d'un exemple du type d'extrait que le collectif sait reprendre à son avantage pour faire clairement apparaître l'échec de la lutte antiterroriste. Ainsi, le collectif tire des médias occidentaux toutes les informations qui vont dans leur sens : une analyse des échecs de la lutte antiterroriste en ligne se transforme en preuve de leur victoire sur le front médiatique.

Conclusion : Visibilité et complexité

Ce chapitre nous a permis de rendre compte de la complexité qui sous-tend l'organisation de la visibilité. Complexe en raison du vaste réseau d'acteurs humains et non-humains qui la sous-tend pour la faire exister. Mais également, complexe dans la mesure où ces entités hétérogènes doivent trouver un équilibre entre les dangers de la technique et le potentiel démocratique d'internet. Rappelons d'abord comment l'État islamique associe internet à un front de bataille. À ce titre, les ambitions assumées du collectif montrent que l'espace numérique doit être déchiffré en termes de guerre. Ce pullulement de métaphores belliqueuses fabriquées par le collectif spécifie une « géographie d'action » (De Certeau, 1990 : 171) qui promulgue des rapports de pouvoir, des stratégies belliqueuses et des rationalités opérationnelles.

[75] *Ibid.*

Cela participe à l'établissement d'un réseau collaboratif d'entités hybrides qui nécessitent des partenariats entre des humains et des non-humains. La guerre ne peut se mener dans l'isolement. Le collectif diversifie ainsi ses acteurs et ses compétences. Il aligne ensemble professionnels des médias, profanes, spécialistes en cybersécurité et *botnets*, pour ne citer que les principaux. En schématisant beaucoup, on peut dire que le collectif privilégie plusieurs pôles d'expérience : celui dont les usages valorisent la convivialité entre les partisans ; et ceux qui inscrivent les usages dans des rapports de conquête et de domination envers ses adversaires.

Par ailleurs, pour mener l'analyse concrète de la visibilité en ligne, nous sommes en mesure de dire qu'il faut complexifier le modèle utopique de l'horizontalité et de la décentralisation. Celui-ci présuppose en effet que les technologies numériques accroissent les capacités d'autonomisation de l'individu. Il serait capable de faire plus par lui-même sans dépendre d'une « quelconque autorisation ou de la coopération d'autrui » (Benkler, 2009 : 38). D'autre part, les technologies numériques laisseraient apparaître un espace en réseau sans centre de contrôle unique et s'affranchissant de modèles de gouvernances plus verticales (Benkler, 2009 ; Castells, 1998). Finalement, comme Castells (2000) l'avance : « by definition a network has no center » (p.15). Or, nous avons démontré comment la visibilité de l'État islamique se négocie dans des routines à la fois centralisées et décentralisées. Internet n'évince pas des modèles plus hiérarchisés et bureaucratiques de production de contenus. Si l'État islamique a été extrêmement efficace dans sa propagande, c'est entre autres grâce à la professionnalisation de ses contenus médiatiques. Ainsi, nous pouvons dire à ce stade qu'internet fait coexister plusieurs formes organisationnelles de production de contenus, tout en juxtaposant une série de médias et de technologies.

Rappelons également que l'utilisateur tend à devenir l'apanage professionnel et technique d'un appareil de production des contenus soigneusement définis et contrôlés. Il devient cet utilisateur fonctionnel qui doit se battre pour une victoire. Le point idéal de cet utilisateur : diffuser le plus de contenus officiels et élargir la portée du message de l'État islamique. À son point extrême, il s'inscrit dans les rouages d'une machination qui lui enlève toute forme d'autonomie et de créativité dans la production des contenus. Sous ce biais, on peut voir que dans les formes contemporaines de distributions de contenu, les humains peuvent s'apparenter à des automates. En pareil cas, les moteurs de cette expansion à l'automatisation sont simultanément incarnés par des agents automatisés, qui deviennent les moyens d'une action

facilitée et plus rapide. Ces rôles fonctionnels participent ainsi à une reconfiguration de la mobilisation en ligne qui se veut davantage automatisée. Par ailleurs, en même temps que les militants et les agents automatisés s'alignent sur la chaîne d'action avec des gestes et actions parfois similaires, ils risquent de brouiller la binarité entre le réel et le faux. L'objectif tant pour les militants que pour les agents automatisés est de se fondre dans le collectif et de servir la cause. Ainsi, ce chapitre accentue deux observations préalables. Premièrement, qu'internet serait de plus en plus pratiqué comme un lieu technicisé. Deuxièmement, qu'il serait un espace hybride. C'est sur cette base que nous alimenterons l'analyse du chapitre suivant.

Chapitre 6 : La mise au travail du collectif et les promesses d'abondance

Le chapitre précédent a été l'occasion de voir comment le collectif transformait internet en un espace de conquête et de domination. Il en ressort des dynamiques collectives et hybrides, des enrôlements, des stratégies, des rationalités et des dramaturgies qui participent à mener la « guerre médiatique ». Cet effort de description d'un espace numérique militarisé ne doit toutefois pas s'arrêter là. Dans ce chapitre, nous continuerons la réflexion amorcée dans le chapitre 5, en nous intéressant cette fois-ci à la façon dont le collectif capte l'attention de ses partisans et de ses adversaires. En d'autres termes, il s'agira d'analyser comment le collectif travaille à attirer le regard de l'autre et les stratégies qu'il utilise pour augmenter sa visibilité. Par ailleurs, ce chapitre mettra également de l'avant les effets politiques et de pouvoir subséquent à ces modèles de visibilité qui, comme nous le verrons, favorisent une abondance d'énoncés. Nous commencerons par décrire la façon dont le collectif manipule sa narration dans des formats numériques qui attirent rapidement l'attention sur les réseaux sociaux. La deuxième partie portera plus spécifiquement sur les stratégies d'amplification mobilisées par le collectif. Enfin, nous verrons comment cette logique d'amplification et d'abondance s'articule dans de nouvelles formes de combats entre adversaires.

6.1. Perpétuer le spectacle : encoder les énoncés en mèmes

Nous avons soulevé dans le chapitre précédent comment le collectif construit un utilisateur fonctionnel, en mettant l'emphase non pas sur ses capacités créatives, mais sur son aptitude à relayer le contenu officiel de l'État islamique. Les partisans n'en perdent pas pour autant un rôle plus actif dans la production des contenus. Plusieurs militants ont élargi et diversifié leur champ d'action en fabriquant de nombreux mèmes. Dans la littérature, les mèmes sont habituellement associés à 4chan[76]. Ce faisant, ils ont majoritairement été dépeints comme produits, pour le *Lulz*, par des hommes blancs hétérosexuels de classe moyenne (Phillips, 2015 ; Nissenbaum et Shifman, 2017). Depuis peu, l'usage des mèmes par des groupes politiques et extrémistes a fait l'objet d'une plus grande attention, comme nous l'avons vu au premier chapitre. Les études intéressées à la fabrication des mèmes par des groupuscules jihadistes sont plus rares. Or, notre enquête montre que le réseau d'énoncés de l'État islamique est constitué de nombreuses opérations qui produisent et reproduisent des mèmes sous différents formats.

Tout au long de notre observation, nous avons été frappés par le nombre d'images macro (images superposées de texte), de GIFs (images animées ou courtes séquences vidéo), d'autocollants[77] et autres créations visuelles en circulation. Fatalement, les contenus générés par les partisans diffèrent de ceux produits par les spécialistes des médias, en ce qu'ils manient cette fois-ci des codes associés à la culture informatique. Ce dernier talent de l'État islamique s'avère être un excellent moyen pour élargir leur cadre visuel et esthétiser la politique. En inscrivant leur narratif dans des formats plus laconiques, ces productions anonymes favorisent inévitablement une attention plus immédiate sur ses contenus et peuvent être une véritable arme de combat (Donovan, 2019 ; Singer et Brooking, 2018).

Les mèmes de l'État islamique jouent sur l'humour, comme c'est le plus souvent le cas avec les mèmes, mais pas seulement. En fait, les mèmes de l'État islamique ne sont que rarement comiques. Ils relèvent au contraire d'une multitude d'autres fonctions. Ils peuvent être ludiques, en diffusant des contenus religieux, servir de base pour le recrutement en multipliant

[76] Le controversé site 4chan est un réseau d'échanges d'images où tout le monde peut publier des commentaires et partager des images de manière anonyme.
[77] Les autocollants sont des éléments graphiques soutenus par la plupart des réseaux sociaux et des applications de messageries. De Seta définit les autocollants comme des « images, usually larger than graphical emoticons and emoji, offered as thematic sets in the communication interfaces of instant messaging apps and social networking services, often organized in tabs and personalized collections » (2018 : para. *Stickers*).

les appels au jihad, ou encore être une arme à l'encontre de ses adversaires en les menaçant directement. Examinons maintenant de plus près les critères permettant le succès de telles opérations.

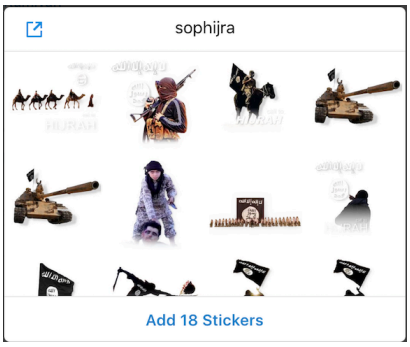

Figure 6.1. Séries d'autocollants créés par l'État islamique disponibles sur Telegram favorisant la grandeur du groupe, sa nature combative et violente.

Figure 6.2. Mème incitant les femmes à se marier avec un *mujâhidîn* en reprenant la formule populaire « keep calm ».

Figure 6.3. Mème humoristique moquant le plan établi en 2017 par le président Donald Trump pour vaincre l'État islamique en 30 jours.

Figure 6.4. Mème qui présente les dirigeants du monde occidental comme les vrais terroristes, contrairement aux jihadistes qui répandent le Bien.

Figure 6.5. Mème signifiant le combat contre l'occident sur fond apocalyptique. La thématique de l'apocalypse est régulièrement reprise par l'État islamique, elle annonce le combat final entre les vrais croyants et les infidèles, entre le Bien et le Mal (El Difraoui, 2016).

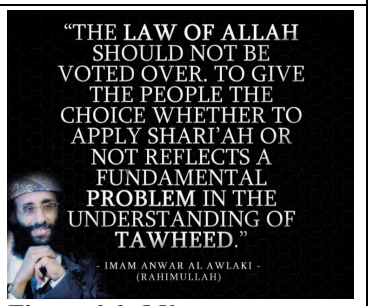

Figure 6.6. Mème mettant en valeur une citation du prédicateur américano-yéménite Anwar al-Awlaqi, mort en 2011 à la suite d'une frappe d'un drone américain au Yémen.

Tableau 6.1. Sélection de mèmes circulant en ligne dans la sphère pro État islamique. Ces mèmes ont été publiés sur les plateformes de réseaux sociaux en 2017 et 2018.

6.1.1. Visibilité et fonction informatique

Le fait que la distribution du visible épouse différents formats découle de la prolifération de logiciels qui permettent de créer et partager facilement des mèmes. Les mèmes sont donc d'abord des objets médiatiques modélisés par des ordinateurs et des logiciels. Il serait excessif de dire que ce sont des biens immatériels, puisque leur fabrication et leur circulation dépendent d'un réseau socio-technique complexe. Face au fait que toutes les étapes de sa fabrication et de sa distribution passent par l'ordinateur, il est difficile d'évincer la strate computationnelle qui la compose. Partant de là, on comprend plus facilement la manière dont la logique de fonctionnement de l'ordinateur s'inscrit dans la modélisation de l'information, mais aussi dans la culture visuelle du collectif.

L'avantage des logiciels qui permettent de produire des mèmes est de rendre possible à tout analphabète du code de devenir un créateur. Le logiciel n'est donc pas un simple point de contact entre un humain et un non-humain. Bien plus que ça, ces « technologies de l'ordinaire » (Aktypi, 2012) pérennisent des savoir-faire réduits et des modes de représentation. Toutefois, il faut un minimum de littératie numérique pour fabriquer un mème. Si la création de ces contenus ne demande pas de compétences en graphisme ou en programmation, elle nécessite pourtant que l'utilisateur crée une base de données et comprenne les fonctions du logiciel.

La base de données peut contenir des références internes ou externes au groupe. En termes plus précis, le militant a le choix de rassembler des contenus provenant de la large bibliothèque du web ou alors de sa propre collection photographiques ou filmiques. Résultat : les mèmes mettent en circulation des objets culturels hétérogènes ou alors se résoudront à un conservatisme en perpétuant les objets culturels du collectif. Cela démontre que le contenu n'est que rarement authentique. À ce titre, Manovich (2010) stipule qu'au sein des nouveaux médias, les contenus sont peu souvent créés ex nihilo. Ils consistent plutôt à assembler et mixer des contenus existants. Cela témoigne du fait que dans la culture informatique, « la création authentique a été remplacée par la sélection qui se fait dans un menu proposé » (Manovich, 2010 : 248).

Une fois la base de données construite et le menu du logiciel déroulé, le partisan est déchargé de la tâche d'assemblage d'éléments sonores ou visuels au sein de la composition, laquelle est

désormais réservée aux algorithmes. Voilà un cas intéressant d'algorithme qui assemble et met en scène des énoncés de manière brève et frappante. Généralement, la littérature s'est limitée à parler du rôle des algorithmes de recommandations des réseaux sociaux, dont le travail est de rendre visible certains contenus au détriment d'autres. Et pourtant, comme nous le voyons, une autre gamme d'algorithmes participe à établir des régimes de visibilité, en circonscrivant des façons de voir. Par les différentes options offertes, ces algorithmes permettent de basculer d'une vue à l'autre et de multiples façons. Nous pouvons maintenant nous demander qu'est-ce que le collectif cherche à nous faire-voir à travers les mèmes ? Allie-t-il conservatisme et création de mèmes ou cherche-t-il à innover ? De manière peu surprenante, le collectif a autant manié la recherche de créativité que la réinscription des contenus officiels.

6.1.2. Le choix du conservatisme : Réinscrire les vidéos officielles en GIF

Le 26 septembre 2017, nous accédons à un groupe Telegram nommé « Caliphate GIFS ». L'objectif de ce groupe, dont l'option de publication pour les autres membres est réduite, est de diffuser des GIFs pro État islamique à l'ensemble de la communauté à des fins de téléchargement et de diffusion. Suite à l'analyse de 75 GIFs téléchargés sur cette chaîne, nous avons pu voir qu'ils suivent tous la même ligne éditoriale : reproduire des séquences ou plusieurs séquences de vidéos réalisées par les médias officiels de l'État islamique.

Ces courtes séquences vidéo rendent perceptibles aux spectateurs des scènes montrant les soldats de l'État islamique lors de combats, d'entraînements et de moments de camaraderies. La fraternité, la bravoure, le courage et le dévouement religieux des soldats apparaissaient ainsi à l'écran le temps de quelques secondes. En plus de cela, ces GIFs pro État islamique sont l'occasion de remettre à l'écran des séquences de décapitation et d'exécution d'otages dans des formats plus succincts. Les séquences sélectionnées sont le théâtre des exécutions en train de se faire. Le noir n'est jamais à l'écran, plutôt, les opérations de montage favorisent l'option du ralenti pour voir les corps en train d'être meurtris dans les moments les plus sordides et sidérants de la violence. Voici les éléments d'une stratégie qui, en exploitant d'autres formats numériques, permet de continuer à « terroriser le cœur des ennemis ».

C'est aussi à travers les GIFs que le collectif fait la gloire des enfants soldats de l'État islamique, surnommés les « lionceaux du califat ». Dans ces recodages, ne circulent que des

séquences d'enfants en train d'effectuer des exécutions, de brandir le drapeau de l'État islamique et dans une moindre mesure d'être formés à des activités religieuses. Ces visuels se livrent à une parade d'enfants militarisés, s'enracinant dans la violence et dans l'idéologie de l'État islamique. Utiliser des enfants est une manière pour le groupe de signaler à ses opposants qu'ils disposent d'une jeune génération pour perpétuer le combat (Benotman et Malik, 2016 ; Vale, 2018). Par ces GIFs, on constate que les partisans de l'État islamique devenaient maîtres d'œuvre dans la réinscription de scènes de violence et d'héroïsme des soldats. Étonnement, alors que les vidéos de l'État islamique couvrent une multitude d'autres thématiques telles que la vie au quotidien et la gouvernance, ces thèmes étaient totalement exclus des GIFs diffusés sur la chaîne Telegram. Le collectif a ainsi essentiellement misé sur la répétition de visuels affirmant leur grandeur et l'état de menace qu'il représente.

On attire ici l'attention du lecteur sur le fait que toute cette machination ne vise pas à innover. Les concepteurs de ces GIFs pro État islamique se contentent d'effectuer des activités de transfert d'un mode d'expression vers un autre. Dit plus simplement, dans ce cas précis, les vidéos de l'État islamique trouvent une nouvelle existence dans un autre format. En cela, le collectif se montre habile en exploitant les capacités de stockage et de réinscription mis à disposition par le dispositif technique. Les possibilités de modularité qu'on retrouve sur internet permettent par conséquent de stabiliser une série d'énoncés en les répliquant et multipliant dans de nouveaux objets médiatiques. On peut y voir un début de régime de mobilité des énoncés, qui dans un contexte où ils sont la cible des suspensions, lui assure en quelque sorte une survie.

6.1.3. Le martyre dans la culture populaire

Pour Guy Debord et Gil Wolman (1956), il existe deux types de détournement. Le détournement *mineur*, qui se limite à détourner des éléments peu importants et dont le sens découle de facto de l'assemblage de ces différents éléments. Ensuite, le détournement *abusif*, qui consiste à redéployer des propositions déjà établies. Lorsque l'objet détourné est rapproché du nouvel élément, il aura une tout autre portée. Incontestablement, ces stratégies de détournements sont facilitées dans un environnement numérique qui valorise la multimodalité, l'intertextualité et la réappropriation (Milner, 2013). Rappelons que l'État islamique est largement composé de jeunes milléniaux et de natifs européens qui ont grandi avec ces technologies et la culture mémétique. Cela a inévitablement eu des répercussions sur

la création des énoncés. Le collectif s'est en effet livré à un jeu d'enchevêtrement combinant culture populaire et jihadisme ; ce qui a donné lieu à un nouveau répertoire d'imagerie.

Des partisans de l'État islamique ont par exemple commencé à réactualiser certains mythes jihadistes à la lumière de codes et esthétismes occidentaux. C'est de ce mélange de genres que naquit une synthèse stylistique entre le mythe du martyre et la culture populaire. Le culte du martyre est central dans la culture jihadiste. Dans une entrevue donnée à CNN en 1997, Ben Laden disait « nous aimons la mort sur la voie de Dieu autant que vous aimez la vie, nous ne craignons rien, nous espérons une telle mort ». Comme Ostovar (2017) le note, « the achievement of martyrdom – to die or be killed in the path of jihad- is considered an honor and a heroic deed by jihadists, who believe that it is afforded by God to only those most deserving of the spiritual bounty » (p.101).

À l'origine, le mythe du martyre a été publicisé par Abdallah Azzam[78], érudit docteur en théologie et père du jihad moderne, dans son texte « *Rejoins la Caravane* ». Dans la conception d'Azzam, le martyre n'était pas associé au kamikaze, mais au *mujâhidîn* mort héroïquement au combat (El Difraoui, 2013). C'est avec Ben Laden et Ayman al-Zawahiri que les opérations suicides ont commencé à se systématiser au sein du jihadisme. Notamment lorsqu'Al-Qaïda a mené plusieurs attentats simultanés contre les ambassades des États-Unis en Tanzanie et au Kenya le 7 août 1988. Le mythe du martyre est devenu un élément central, voire fondamental dans le récit d'Al-Qaïda. Ce mythe a largement été repris ensuite par Abu Mussab al-Zarqawi.

Cook (2017) explique que la contribution d'Abu Mussab al-Zarqawi à la culture jihadiste est d'avoir repris des récits mythiques édictés par Ben Laden et d'autres dirigeants salafistes-jihadistes qui dépendait alors largement de la télévision, pour les replacer dans l'environnement du web. Par exemple, au fur et à mesure de son intégration dans l'environnement numérique, le mythe du martyre s'est inscrit dans une cosmologie plus large et éloignée des productions audiovisuelles contrôlées d'Al-Qaïda. Il était retravaillé dans plusieurs formats visuels, au point que les mèmes sont devenus des « blocs » supplémentaires à la construction du mythe du martyre. Un répertoire symbolique qui permet de séduire un

[78] Malgré que la notion de martyre ait occupé une place abondante dans la théologie médiévale, elle reste peu évoquée dans les écrits islamistes antérieurs à Azzam. C'est seulement après Azzam qu'elle est devenue la « marque de fabrique » des groupes islamistes radicaux (Hegghammer, 2005).

public plus transnationalisé et juvénile, s'est ainsi forgé. Prenons deux exemples qui montrent comment les partisans ont réussi à aligner culture populaire et jihadisme.

Exemple #1 : YODO

Les partisans ont manifestement été inspirés par un slogan qui fut très populaire sur les réseaux sociaux : YOLO (You Only Live Once). YOLO a été largement utilisé comme *hashtag* sur Twitter pour décrire des événements excitants ou risqués, après avoir été popularisé par le chanteur Drake dans son single « The Motto ». Les partisans de l'État islamique ont opéré un double détournement de cet acronyme. Premièrement, ils ont combiné l'acronyme YOLO avec un appel au jihad. Deuxièmement, ils ont transformé YOLO en YODO (You Only Die Once) pour promouvoir la voie du martyre. Ainsi pouvait-on lire : « You only die once why not make it martyrdom ». En inscrivant le mythe du martyre dans la culture populaire, le collectif inverse comme dans un miroir la polarité de la Vie et de la Mort, en transformant la Mort en signe positif et en gage de plénitude. Sur fond militarisé, YOLO – servant de prime abord à persuader de profiter de la vie – cristallise dès lors des croyances mortifères.

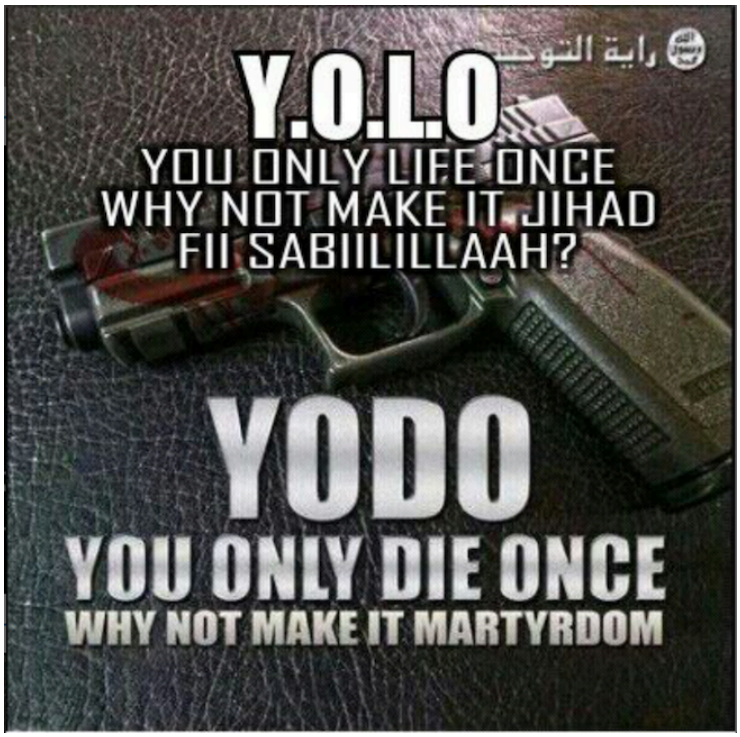

Figure 6.7. Mème pro État islamique faisant la promotion du jihad et martyre en détournant l'acronyme YOLO, publié en 2017 sur Telegram.

Exemple #2 : Quand Mario devient un kamikaze

Mario est le protagoniste du jeu vidéo Super Mario créé par Nintendo en 1985. Mis en scène dans le Royaume Champignon, il faudra le faire progresser à travers plusieurs niveaux. À cette icône du jeu vidéo, les partisans de l'État islamique ont donné une nouvelle histoire. En fabriquant un nouveau GIF, le but était de superposer à Mario le mythe du martyre. La scène commence par Mario sautant sur un mur de pierre, pour ensuite brandir l'étendard de l'État islamique. Il se dirige dans un troisième temps vers une maison en brique où il commet une attaque-suicide pour mourir en martyre. Mario s'est ainsi vu offrir une interprétation mortifère. Entre autres choses, il incarnait ce qu'il y a de plus terrifiant pour l'adversaire : les opérations-suicides. En partant de figure mythique de la culture populaire, il s'agit aussi de montrer que l'acte de martyre est accessible à tous et est étrangement contemporain.

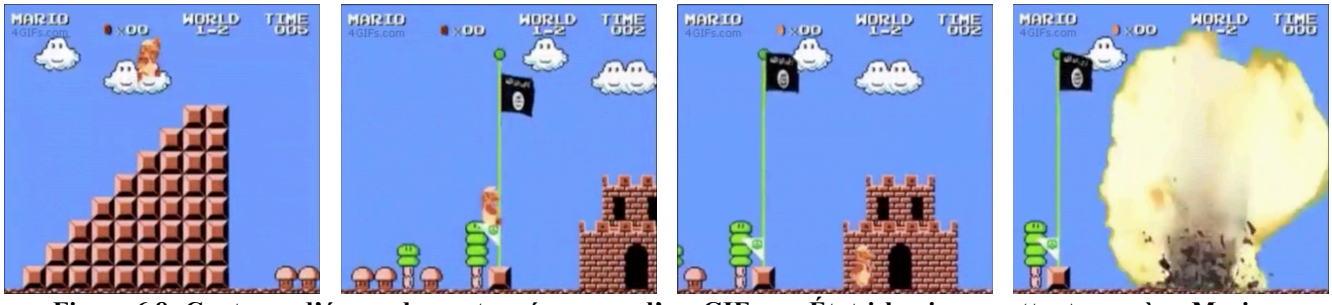

Figure 6.8. Captures d'écran de quatre séquences d'un GIF pro État islamique mettant en scène Mario dans une opération-suicide. Ce GIF a été publié en 2017 sur Telegram.

La culture jihadiste a ainsi été profondément influencée par la culture populaire des jeunes milléniaux. Cette nouvelle vague de partisans de l'État islamique a hérité de la culture informatique et de son goût pour la réappropriation, la multimodalité et l'humour. Les mythes forts du jihadisme sont ainsi devenus des éléments hybrides de deux cultures qui n'ont en apparence rien en commun. De façon générale, que le mème jihadiste soit innovant ou non, nous pouvons dire qu'il est un dispositif de communication qui simplifie le récit politico-religieux du collectif. Simultanément, il accélère sa vitesse de propagation au sein de publics variés en étant facilement partageables. Une stratégie sans conteste saillante pour le groupe. L'exemple des mèmes nous permet également de conclure que « the boundaries of jihadist visual culture are not fixed » (Ostovar, 2017 : 107). Nous voyons bien ici, comment des utilisateurs se réapproprient et détournent des éléments de la culture populaire pour l'intégrer dans une trame visuelle jihadiste.

6.2. Amplifier la protestation : Stratégies et manipulations

Ainsi que nous l'avons souligné précédemment, le cœur de la mission de l'État islamique est d'envahir le web. Dans cette optique, l'aspiration de l'État islamique est de distribuer ses énoncés le plus largement possible. Pour ce faire, le collectif a appris à optimaliser et manipuler les technologies du web. Les sections suivantes déplient ces stratégies d'amplification en mobilisant différents exemples : celui de la fonction @Reply, du *hashtag* et de la création de fausses amplifications. Nous verrons aussi comment ce programme d'amplification et d'abondance s'est traduit dans la construction d'un imaginaire technisiste qui se manifeste dans la précision et l'harmonie des agencements.

6.2.1. Fonction @Reply : L'exemple des attentats

Nous sommes le 1er octobre 2017, un homme, Stephan Paddock, tire du 32e étage de l'hôtel Mandalay Bay Resort and Casino à Las Vegas sur une foule assistant à un festival de musique country en plein air. L'attaque est rapidement revendiquée par l'État islamique. Une revendication que la police locale et le FBI ont toujours réfutée, n'ayant établi aucun lien formel entre Stephan Paddock et un quelconque groupe jihadiste[79]. Toutefois, le collectif maintiendra sa version des faits et célébrera l'événement comme une victoire sur ses adversaires. Comme pour chaque attentat, le collectif travaille ardemment à produire des énoncés officiels et non officiels pour publiciser autant que possible l'événement. Cette production intensive d'énoncés marque leur volonté de capter entièrement l'attention accordée à l'attaque.

Parmi les comptes Twitter pro État islamique actifs ce jour-là, surgi l'utilisateur @imnjlloxyrk67icj. La mise en forme du profil indique directement le rôle qu'il compte jouer : donner le plus de visibilité possible à l'attaque. Cela commence par sa photo de profil, qui est celle de l'auteur de la fusillade[80]. Ensuite, la bannière du compte, qui affiche la façade de l'hôtel. À ce stade, tout évoque la fusillade qui venait d'avoir lieu. Comme il est

[79] La revendication du groupe État islamique a posé de nombreuses questions. Quelques heures après la fusillade, le groupe a revendiqué la tuerie via l'agence A'maq, en présentant Stephen Paddock comme l'un des ses « soldats » et dans un deuxième communiqué précisant qu'il s'était converti il y a quelques mois à l'islam. Wassim Nasr, journaliste spécialiste des questions jihadistes a déclaré sur France info « Pour Las Vegas, si c'était une revendication farfelue, ce serait une première ». Voir : https://www.francetvinfo.fr/monde/usa/fusillade-a-las-vegas/fusillade-de-las-vegas-pourquoi-la-revendication-du-groupe-etat-islamique-pose-question_2399902.html

[80] Mettre l'assaillant en photo de profil lors d'attentats commis en occident est une pratique courante chez les partisans de l'État islamique.

coutume de l'observer, le compte a peu d'abonnés et d'abonnements. Là, n'est pas le but. L'une des seules et uniques fonctions de cet utilisateur est de solliciter sur Twitter les adversaires de l'État islamique et de distribuer mécaniquement des *tweets* qui propagent l'événement. Une opération tactique rendue possible par la fonctionnalité Twitter @Reply (composée du signe @ et du nom d'utilisateur). Celle-ci « lets users target a conversation to or reference a particular user, but these *tweets* can be viewed by anyone through search.twitter.com, the public timeline, or the sender's Twitter page » (Marwick et boyd, 2010 : 117). Dans les faits, elle permet de dépasser « l'audience imaginée » (Marwick et boyd, 2010) en s'adressant directement à des utilisateurs.

Pour mener à bien son projet, @imnjlloxyrk67icj a commencé par accomplir un travail de mise en scène des énoncés. Clairement, ce qu'il vise est une guerre psychologique. La menace et la terreur passent au premier plan de la stratégie communicationnelle de @imnjlloxyrk67icj, comme en témoigne ce *tweet* : « The war has just begun! More deadly attacks are coming! One day the #IS flag will be raised in your seat of Power the White House! ». Au second plan, l'utilisateur mobilise un registre de justification, en attestant qu'il s'agit d'une revanche face aux bombardements de la coalition internationale. Cela fait écho à ce qu'indique Arendt dans son ouvrage *Du mensonge à la violence*, à savoir que « la violence recherche toujours une justification » (1972 : 177). Pour donner le plus possible de consistance à ses *tweets* @imnjlloxyrk67icj, le texte combine des communiqués officiels revendiquant l'attentat, des mèmes célébrant l'attaque et l'assaillant et des images d'enfants victimes de bombardements de la coalition.

Une fois le récit condensé dans une série de textes et d'images, il lui faudra cibler les utilisateurs. @imnjlloxyrk67icj a principalement pris pour cible des agences de presse américaines et internationales, ainsi que le compte Twitter POTUS (acronyme pour President of the United States of America). La manière dont @imnjlloxyrk67icj procède est de répondre à un Tweet posté par l'un de ces comptes. Les exigences pour faire transiter les énoncés au sein de ces audiences sont simples : propager le plus de publications relatant l'événement. La chaîne peut être allongée autant qu'elle le pourra, en multipliant les @Reply et en se résolvant à s'immiscer dans une panoplie de discussions touchant à la fois les informations sur la fusillade que des *tweets* qui n'avaient aucun rapport avec l'événement.

Figure 6.8. Exemple de mème diffusé lors de l'attaque de Las Vegas. On y voit une photo de l'assaillant Stephan Paddock, auquel a été ajouté son nom de guerre. Le visuel fait aussi état des résultats de l'attaque en termes de morts et de blessés.

Si @imnjlloxyrk67icj n'a pas spécialement cherché à interpeller des comptes d'utilisateurs peu populaires, il n'en demeure pas moins que pour d'autres partisans de l'État islamique, il s'agissait d'un choix privilégié. C'est par exemple le cas de @bskx_glfs, qui a ciblé de nombreux utilisateurs ayant utilisé le *hashtag* #SaintPertersbourg lors de l'explosion de son métro en avril 2017. Ce *hashtag* avait été principalement créé pour exprimer une solidarité avec les victimes de l'attentat. Malgré que l'attentat n'ait pas été revendiqué par l'État islamique, pour les partisans c'était l'occasion de réactualiser l'état de menace.

> <@Canines_xvxs> #SaintPetersbourg local media obtains images of the metro bombing suspect #CNN BREITBART @FoxNews
>
> <@bskx_glfs> please join to Islam religion before Beheading from our soldiers of Islamic State in Near Your Home Town. (Échange Twitter, 3 avril 2017)

Il n'est pas sans intérêt de regarder maintenant d'un peu plus près si la fonction @Reply a suscité un engagement de l'internaute interpellé par le partisan de l'État islamique. Nos

observations montrent que la réaction de la presse et du public aux provocations des partisans de l'État islamique restait tout bonnement silencieuse. Cela peut relever deux hypothèses. Premièrement, ces narratifs impliquent une réalité brutale et violente difficile à commenter. Deuxièmement, les *tweets* se perdent tout simplement dans le flux informationnel. Cette dernière hypothèse est tout à fait plausible, en particulier pour les comptes générant une large audience telle que le compte Twitter POTUS ou des agences de presse réputées. La fonction @Reply ne réalise donc pas un dialogue effectif. Dans les rares cas où le *tweet* du partisan de l'État islamique provoquait une réaction, l'échange était extrêmement court, peu argumentatif, surenchérissait les menaces, et sans grande originalité se contentait de republier les mêmes *tweets* que préalablement.

Lorsque, par exemple, @imnjlloxyrk67icj a interpellé le compte du média Reuters, qui publiait des informations sur la fusillade de Las Vegas, un utilisateur indiquant dans sa bio avoir « served this nation in the USAF for 20 years », s'est immiscé dans l'échange. Ce dernier a notamment répondu à @imnjlloxyrk67icj en publiant le *tweet* suivant : « FUCK ISLAM, FUCK MOHAMED AND FUCK YOU ! » et en y joignant l'image suivante :

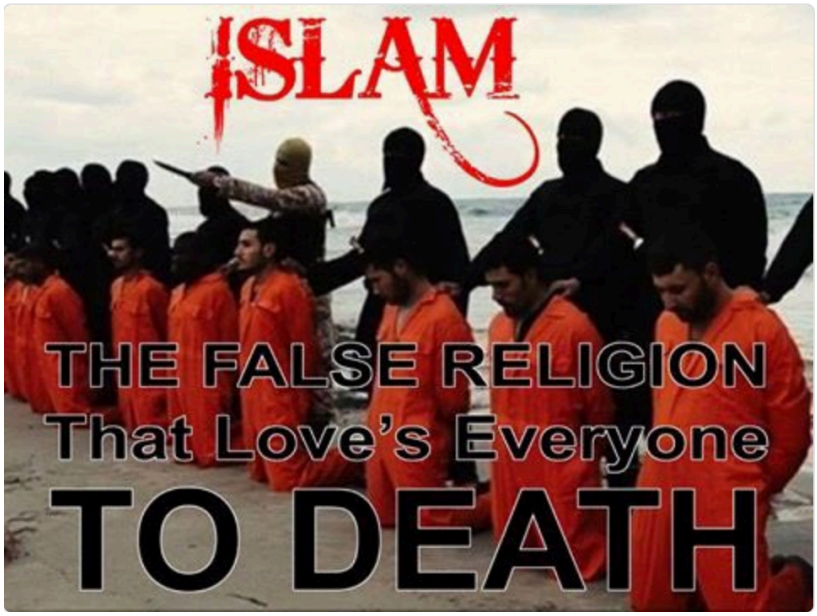

Figure 6.9. Mème posté par un opposant à l'État islamique dans le cadre d'une interpellation d'un militant pro État islamique à l'égard du média Reuters.

@imnjlloxyrk67icj a simplement répondu en postant le communiqué officiel de l'État islamique « About 600 people were wounded and injured from the crusaders in a blessed attack in the American city of Las Vegas ». À cette réponse, l'utilisateur a republié le même visuel (figure 6.9). @imnjlloxyrk67icj surenchérira avec un autre communiqué de l'agence de

propagande A'maq indiquant « Las Vegas attacker is a soldier of the Islamic State who carried out the attack in response to calls for targeting coalition countries ». Fin de l'interaction.

Nous pouvons ainsi constater que si la fonction @Reply est productive quand il s'agit de distribuer le contenu à des audiences variées, elle présente des limites lorsqu'on s'intéresse à elle sous tous ses angles. Si cette fonctionnalité informatique est capable d'établir une liaison entre des internautes, la fonction @Reply est dans ce cas-ci peu propice à un usage conversationnel. Elle est au contraire révélatrice de tactiques de *trolling*[81] qui visent à semer la controverse, à harceler des utilisateurs et à perturber l'équilibre de la communauté. Voici des opérations qui nous éloignent de l'idéal d'interactivité et de convivialité promue par les plateformes et les cyber-utopistes.

6.2.2. #Hashtag et tendances sur Twitter

Une façon différente d'attirer l'attention sur le collectif implique un autre type d'entité non-humaine : le *hashtag*[82]. Les *hashtags* sur Twitter ont cette double fonction de permettre la recherche de contenu sur la plateforme et de fournir des moyens de hiérarchiser l'information. Les *hashtags* qui bénéficient d'une grande popularité ont de plus grandes chances de se retrouver dans les « tendances » de Twitter. Ce « système d'indexation » (Bonilla et Rosa, 2015) donne lieu, de ce fait, à une surenchère formelle des informations. En d'autres termes, pour atteindre le statut d'*hyper-visibilité*, les *hashtags* sont continuellement en compétition les uns avec les autres. Au point de jonction de cette visibilité se trouve l'algorithme, sans lequel la hiérarchisation et l'opérationnalisation des tendances sont impossibles.

Ce calculateur numérique quadrille des façons de voir qui seront à la fois personnalisées et immédiates. Plus précisément, chaque compte d'utilisateur se voit assigner des tendances

[81] Ces pratiques d'abord utilisées et popularisées par Anonymous, ont été décrites par Gabriela Coleman (2016) ou encore par Witheny Phillips (2015). Le *troll* est un « internaute qui intervient dans le seul but de nuire en soulevant la polémique, souvent en insultant des groupes ou des individus, pour le simple plaisir de la chose » (Coleman, 2016 : 470). Des pratiques qui comme le cas l'atteste se sont généralisés à d'autres groupuscules et pour d'autres raisons.

[82] Le terme *hashtag* sur Twitter a été inventé en 2007 par le designer Chris Messina. Il s'agit d'un mot valise qui supporte les mots « hash » et « tag ». Le caractère croisillon (#) qui lui est associé est un symbole important pour « marquer » les sujets (Mina, 2019). Cette fonctionnalité n'est toutefois pas singulière à Twitter. Déjà en 1990, sur l'Internet Relay Chat, un système de chat open source, les noms des canaux étaient préfixés d'un # pour que les utilisateurs puissent plus facilement les retrouver. Au sein de la culture numérique, le # s'est ainsi généralisé pour organiser l'information au travers de sujets et d'événements particuliers (Mina, 2019 ; Small, 2011).

personnalisées, selon ses abonnements, ses centres d'intérêt et sa localisation. En outre, voulant offrir une expérience en temps réel à ses utilisateurs, les algorithmes de Twitter cibleront les sujets populaires à l'instant T, plutôt que ceux qui le sont depuis quelque temps ou tous les jours. Cette visibilité prend donc appui sur un système de hiérarchisation permanent, en assignant de manière personnalisée aux utilisateurs ce qu'ils doivent voir. Il apparaît assez clairement que les utilisateurs ne voient donc pas les mêmes choses sur la plateforme.

Le collectif a su profiter de ce nouveau lien matériel avec le dispositif technique pour distribuer ses énoncés. Favorisant la circulation de l'information, les *hashtags* sont rapidement devenus un véhicule important pour propager leur contenu. Dans un espace où leur visibilité est contrainte par les effets de la modération, le *hashtag* est une médiation utile qui leur permet d'intensifier la distribution de leur contenu. Grâce au *hashtag*, le collectif n'a pas besoin d'avoir un nombre important d'abonnés pour diffuser son message, puisqu'il lui permet d'avoir un impact au sein d'une large foule d'utilisateurs. De plus, les *hashtags* ne sont pas supprimés ou bloqués par Twitter. Si nous prenons le *hashtag* extrêmement viral produit par l'État islamique en 2014 #AllEyesOnISIS, nous pouvons constater à ce jour qu'il existe toujours sur la plateforme, même s'il a fait l'objet de nombreux détournement pour moquer le collectif.

Ainsi, en se mêlant au collectif, les *hashtags* ouvrent au collectif un champ de possibilité pour accroître leur visibilité, au point que son utilisation est devenue une sorte d'obligation informelle au sein des militants. C'est par exemple ce qu'en témoigne un bref échange paru sur Twitter en septembre 2017 entre deux partisans de l'État islamique. Lorsque l'utilisateur @yxyklyz23432 a publié un Tweet faisant l'apologie d'attaques terroristes, l'utilisateur @rk41ru23 lui a rappelé que l'usage de *hashtag* est une tactique essentielle pour atteindre une plus large audience :

<@rk41ru23> Share it in #hashtag to be seen by all those who are on Twitter

À la suite de quoi, @yxyklyz23432 publiera le même *tweet* en y ajoutant une longue chaîne de *hashtags* (malgré que Twitter recommande de ne pas utiliser plus de deux # par *tweet*) qui n'avaient pas grand-chose à voir entre eux :

<@yxyklyz23432> Strike their necks wherever you can ! #usa #isis #ThursdayThoughts #MorningJoe #PeaceDay

La répartition des hashtags

Pour maximiser l'usage stratégique des *hashtags*, le collectif a mis en œuvre plusieurs stratégies. 1° *Indexer un répertoire de mots-clés qui fait directement référence aux aspects idéologiques, politiques et théologiques de l'État islamique*. Ces médiations textuelles ont l'avantage de fournir des référents sémantiques collectivement partagés par l'État islamique. Ils permettent une synchronisation lexicale qui sort le partisan de son isolement en le rattachant à une identité collective. Il est équipé d'un répertoire de mots-clés qui n'ont d'autres fonctions que de constituer un centre d'attention qui organise et relate l'idéologie du groupe.

Ces dénominateurs communs s'articulent sous différentes formes. Ils peuvent renvoyer directement au collectif #IslamicState (un *hashtag* devenu plus utilisé par journalistes, analystes et adversaires), #The_global_campaign_to_support_the_Islamic_State ; à des slogans populaires #Baqiya[83], #Caravans_of_Martyrs ; à une manière de nommer l'adversaire #Nusayri pour faire référence au régime syrien, #Crusaders pour la communauté internationale ou encore #Rafidi pour les chiites. Enfin, certains *hashtags* font référence à tout leur arsenal de centres médiatiques comme #Amaq, #AlHayatMediaCenter, #BayanRadio, etc., et permettaient de faire circuler leur dernière production, par exemple #Rumiyah ou encore #Dabiq.

2° *Utiliser des hashtags à tonalité neutre*. N'oublions pas que l'État islamique cherche à s'établir territorialement et qu'il a contrôlé un vaste territoire s'étalant de la Syrie à l'Irak pendant ses années de gloire. Le collectif a fait un usage abondant des *hashtags* renvoyant aux zones géographiques qu'ils détenaient et où il combattait. Il va sans dire qu'il s'agit pour le collectif d'une méthode efficace pour joindre en temps quasi réel ses nouvelles militaires au flux informationnel plus large concernant la province en question. Le collectif associe ce type d'*hashtag* à des communiqués officiels, des reportages photos ou des vidéos, aux dommages et victimes des bombardements de la coalition ou encore à des menaces directes envers

[83] Il s'agit d'un slogan largement utilisé par l'État islamique. Il signifie « il restera ».

l'ennemi. Illustrons rapidement comment le collectif utilise sur le long terme un même *hashtag* pour y joindre différents narratifs :

- Targeting Vehicles of the #Rafidi Federal Police with Rocket Projectiles in the Outskirts of the Area of Bab at-Tub in the Right Side of #Mosul (Twitter, 15 mars 2017)

- Mass torturing of Sunni civilians in #Mosul by US & European supported by Iraqi police (Twitter, 14 juillet 2017)

- #Mosul NO PLACE FOR RAFIDIS IN THE LAND OF THE CALIPHATE (Twitter, 18 mars 2017)

Cet intermédiaire textuel représente ainsi un catalyseur efficace pour articuler différents types de narratif.

3° *Détourner les hashtags*. Pour accroître leur impulsion belliqueuse et leur pénétration au sein d'audiences variées, le collectif fait un usage abondant des *hashtags* tendances et populaires. En juxtaposant ces *hashtags* à son matériel de propagande, il obstrue l'attention existante et ce qui est en vogue. C'est ici que pour assurer la transmission de ses énoncés, l'utilisateur trahit le dispositif technique. Il est totalement prohibé par Twitter d'utiliser un « hashtag tendance ou populaire dans le but de subvertir ou de manipuler une conversation, ou de générer du trafic ou d'attirer l'attention sur des comptes, des sites web, des produits, des services ou des initiatives », ainsi que de créer des « Tweets contenant des *hashtags* excessifs et sans rapport ». Un mésusage que la plateforme associe à une posture de *spammeur* [84].

Pour performer au mieux ce rôle de *spammeur*, des actions sont mises en œuvre pour fournir aux partisans les *hashtags* les plus populaires. C'est face à cet objectif que des chaînes Telegram spécialisées dans « l'invasion » des réseaux sociaux sont apparues. Ces chaînes listent des *hashtags* tendance sur Twitter, ce qui nécessite inévitablement un travail de veille. En d'autres termes, le dispositif technique est scruté pour organiser des campagnes synchronisées. Ces chaînes s'organisent de manière à promouvoir les *hashtags* tendance selon les pays. Ainsi pas moins d'une quinzaine de pays pouvaient être ciblés : États-Unis, Italie,

[84] Le *spammeur* est associé à celui qui vise à amplifier ou à supprimer artificiellement les informations, ou d'adopter un comportement qui manipule ou perturbe l'expérience des utilisateurs. Voir Twiter : Politique en matière de manipulation de la plateforme et de spam https://help.twitter.com/fr/rules-and-policies/platform-manipulation

France, Allemagne, Turquie, Arabie saoudite, Émirats arabes unis, Indonésie, Oman, Qatar, Égypte, Jordanie, Koweït, Algérie, Bahreïn ou des catégories plus larges comme « World ».

Les partisans s'emparent-ils de ce travail effectué en amont pour faire circuler les énoncés ? Difficile à dire. Les chaînes que nous avions rejointes se soldaient d'un faible succès par rapport à d'autres. Elles ne gagnaient pas le groupe dans son ensemble. De plus, lorsque nous copions-collons les *hashtags* diffusés par ces chaînes, nous ne trouvions généralement pas de *tweets* reliés à l'État islamique. Si certaines publications ont pu se perdre dans le flux informationnel, nous étions loin de l'invasion espérée par ce type de chaîne. Quoi qu'il en soit, efficacité ou non de ces chaînes, il est un fait incontestable : les partisans font un usage abondant des *hashtags*. Certes, ils n'inonderont jamais littéralement un *hashtag* tendance comme le fantasme le collectif, toutefois, ces mots-clés sont son équipement. Ils arment le militant à *spammer* le plus grand nombre des flux informationnels et à donner à leurs publications une plus grande visibilité.

En résumé, les énoncés viennent transformer ou stabiliser le sens d'un *hashtag*. Ils le traduisent et retraduisent, l'entremêlent dans un nouveau récit. Le *hashtag* est quant à lui un intermédiaire de plus pour le collectif, qui allongent le réseau initial de production et de distribution des énoncés. Il est un centre d'attention qui capitalise et matérialise le déplacement des énoncés. Il est une arme efficace, en ce qu'il est durable, transposable et reproductible. Il peut agir simultanément dans différents contextes. Il synchronise plusieurs traductions en même temps, sans imposer aucune limite sur les énoncés hétérogènes qui lui sont associés.

6.2.3. La fabrique des fausses amplifications

Dans ces formes d'organisation qui favorisent l'abondance, les militants ont poussé aussi loin que possible la manipulation des plateformes pour réaliser leur programme d'action. C'est dans ce contexte qu'ont émergé des chaînes Telegram spécialisées dans la fabrication de *tweets* opérationnels, de telles sortes qu'ils puissent ensuite être copiés-collés par des militants sur Twitter. Pour que le scénario fonctionne, les mêmes non-humains doivent continuellement s'aligner. Un *tweet* opérationnel se constitue d'un dispositif qui établit des branchements entre du texte, des liens URL et des *hashtags*. On y voit des énoncés pro État islamique qui ne dépassent pas 280 caractères, des *hashtags* et des liens URL de comptes Twitter qui se nouent

dans un destin commun : accumuler les inscriptions pro État islamique au sein de Twitter ou pour reprendre les termes du collectif, provoquer des « Twitter Storm ».

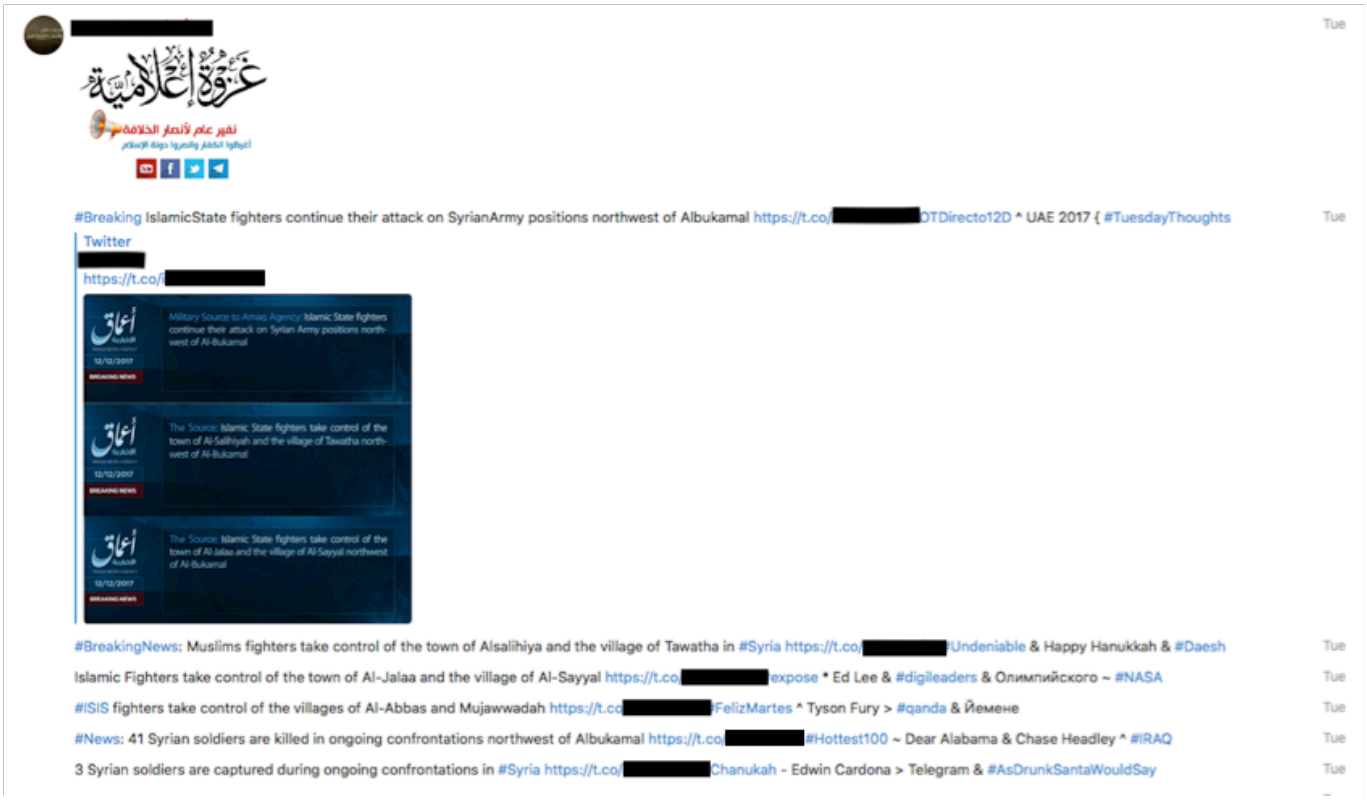

Figure 6.10. Exemple de structure de Tweets opérationnels à partir d'un communiqué de l'agence de presse Amaq. On y voit *hashtags*, textes et lien URL vers le compte Twitter Ashhad qui assurera la transmission du visuel produit par l'agence de presse Amaq. Capture écran datant du 13 décembre 2017.

Observons de plus près les comptes Twitter attachés aux *tweets* préfabriqués. Ces comptes Twitter sont spécifiquement dédiés au stockage du matériel médiatique de l'État islamique. On y retrouve des productions anciennes et nouvelles, des contenus officiels ou non, ce qui démontre que tout type d'inscriptions peut servir de bases opérationnelles. Il est un fait que la diffusion des derniers communiqués et productions officiels de l'État islamique est privilégiée. En quelque sorte, ces comptes Twitter doivent mettre en relief les traces énonciatives du collectif et leur permettre de voyager au sein de différents espaces. Il demeure que les concepteurs de ces comptes lui assurent la fonction la plus instrumentale possible. Il ne faut pas reconstituer l'histoire d'une identité militante au travers du profil. La photo de profil est celle de Twitter par défaut. Leur nom et pseudonyme est habituellement une suite de lettres. Aucun abonnement et abonné. Seuls figurent les communiqués et les productions de l'État islamique. Il se présente ainsi sous la forme d'un dispositif de stockage et de réserve du matériel médiatique.

En enrichissant le stock de publications des militants, les administrateurs de ces chaînes espèrent que les partisans se conforment au scénario initial. Deux types de consignes comparaissaient sur ce type de chaîne. La première est de copier-coller les *tweets* directement sur Twitter. La seconde est d'infiltrer et d'harceler d'autres comptes sur Twitter, comme en témoignent les instructions de la chaîne Telegram :

> Copy the following tweets and enters them directly to the targeted accounts below, then go to the last tweet for each account and post a reply.

À la suite de ce message, suivait une liste de plusieurs dizaines de comptes Twitter sélectionnés. Les principales cibles étaient les agences de presse américaines et internationales. Les comptes de Donald Trump et d'Hillary Clinton étaient également ciblés, ou encore de personnalités connues telles que Jimmy Kimmel, Kanye West, Oprah Winfrey, voire même des clubs de football comme le Real Madrid.

Se dessine dès lors un schéma d'action qui propose une assistance dans le travail de diffusion. Elle s'articule dans une myriade de lieux qui nécessite une collaboration entre dispositifs techniques et humains. Le travail de distribution est partagé entre des personnes ou des services considérés comme des « concepteurs », des « stocks » et des « diffuseurs ». L'action comprend donc des bâtisseurs et des exécutants qui s'articulent au sein de trois catégories d'opérateurs. Premièrement, les concepteurs qui programment et assemblent les énoncés. Deuxièmement, l'encadrement technique chargé de faire appliquer le scénario grâce à différentes technologies web. Troisièmement, les exécutants chargés de suivre le plan. C'est cette troisième catégorie d'acteurs qui permettent de lancer le fonctionnement du scénario. En somme, lorsque ces derniers s'exécutent à la tâche machinique du copier-coller, que nous pourrions résumer comme la « tâche machinique du clic ».

Les résultats de cette tactique dépendent donc de la dimension collective de cette opération et plus particulièrement de la couche de « diffuseur ». En d'autres termes, pour garantir le succès de ces campagnes médiatiques il faudra effectivement un nombre suffisant de militants pour propager les *tweets* préfabriqués. Cela démontre l'image que se font les administrateurs de ces chaînes à l'égard des autres partisans : un internaute disposé à mouvoir cette masse croissante d'énoncés. Or, se joue ici une véritable fracture entre l'internaute-partisan qu'il projette et l'internaute-partisan réel. Nos observations montrent que peu d'utilisateurs s'impliquent

réellement dans ces campagnes de diffusion. Sur les nombreux comptes Twitter pro État islamique que nous avons suivis pendant notre enquête, ces derniers avaient tendance à publier de façon autonome, c'est-à-dire sans se rattacher à une préfabrication de *tweets* qu'ils auraient tout simplement à copier-coller. Cela marque un échec de la tâche machinique du clic humain.

L'entrée en scène du robot

La source immédiate de la diffusion de ces *tweets* opérationnels n'est pas celle de la propension de l'homme à exécuter cette tâche, mais de sa capacité à déployer des *botnets*. La particularité des *botnets* de l'État islamique est qu'ils ressemblent plus à des comptes *spam* qu'à des profils qui chercheraient à avoir une apparence humaine. Ses concepteurs minimisent ainsi la personnification de la machine, malgré les nombreuses ressources qui existent pour la conception de ce type d'interface. L'apparence du compte témoigne d'une extrême simplicité. Ces comptes ont souvent les caractéristiques suivantes en commun : ils affichent la photo par défaut de Twitter, ne présentent aucune information dans la section biographie ni aucune métadonnée de géolocalisation, et ont rarement des abonnés et des abonnements. Chaque botnet opère sous une simple suite de chiffres et de lettres ou alors sous de faux noms générés aléatoirement. Toutefois, il arrivait que leur nom soit plus évocateur, comme « chevaliers-invasion » ou « chevaliers des tempêtes ».

Plutôt que de créer de fausses nouvelles ou de nouveaux contenus, les *botnets* de l'État islamique ont pour but d'amplifier les *tweets* préfabriqués. Ainsi, ces agents automatisés ont principalement été actifs dans la publication des *tweets* opérationnels et dans leur *retweet*. Ils ont également été programmés pour les propager auprès d'utilisateurs ciblés, en faisant un usage abusif de la fonctionnalité mention et réponse. Pour mener l'action, les *botnets* sont subdivisés en plusieurs sous-réseaux de faux comptes automatisés et ont des modèles de spécialisation précis : certains se consacrent à une tâche bien précise, comme le *retweet* par exemple, quant à d'autres ils adoptent des schémas d'actions mixtes où plusieurs fonctionnalités peuvent s'entrecroiser.

Ainsi, ces programmes informatiques sont peu sophistiqués et ne cherchent pas à imiter ou cloner le comportement humain. Ils s'apparentent plus généralement à des comptes *spam*, en dupliquant des *tweets* identiques avec des liens ou non relatifs au matériel médiatique de

l'État islamique. Cette automatisation correspond à ce que Simondon (1958) assimile à un degré de perfection technique extrêmement bas. Dès lors, on peut se représenter les *botnets* du collectif comme des substituts et des perfectionnements artificiels, qui renonçant à certains fonctionnements et usages, ne requièrent d'aucunes marge d'indétermination. Or, l'indétermination, qui peut être retrouvée dans des modèles plus complexes d'apprentissage automatique de certains *botnets*, est pour Simondon ce qui caractérise le degré de technicité d'un dispositif.

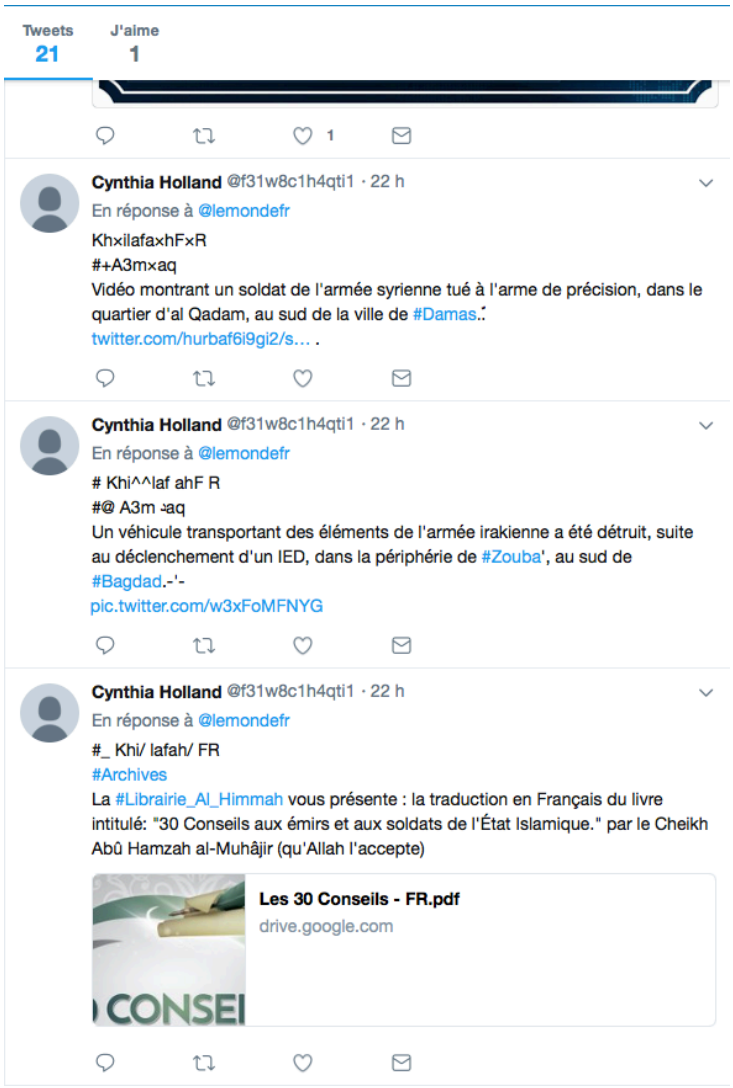

Figure 6.11. Exemple du compte suspect Cynthia Holland qui mène une campagne de harcèlement auprès du quotidien français Le Monde. Ces *tweets* ont été publiés le 21 mars 2018.

En examinant plus en détail comment les *botnets* interagissent avec le « monde extérieur », nous avons pu remarquer que chacun des réseaux de *botnets* fonctionne en système clos. Sauf dans les cas où les *botnets* font usage de la fonctionnalité réponse et mention pour cibler des utilisateurs, ces derniers n'interagissent qu'au sein de leur réseau. En somme, un tweet généré

par un bot n'est *retweeté* ou aimé que par les autres *botnets* du sous-système et en aucun cas par des humains. Tout comme, à l'inverse, les *botnets* ne *retweetent* pas des publications générées par des humains. Alors que des publications pro État islamique produites par des humains peuvent susciter des réactions tant de la part d'autres militants que de ses adversaires, ce n'est pas le cas pour des *tweets* généré par les *botnets*. Cela démontre que dans ce contexte particulier, l'interaction machine-humain se solde par un échec.

Toutefois, si ces agents automatisés ne provoquent pas un engagement direct et tangible avec des humains, ils seront susceptibles de jouer un rôle dans l'expérience humaine. Ces artefacts qui diffusent l'idéologie du groupe au sein de la plateforme permettent une accumulation toujours plus importante des énoncés de l'État islamique. Les *botnets* traduisent des actions spécifiques qui permettent à l'humain de voir et de lire un ensemble de publications relatives au collectif. Ils lui offrent une représentation d'un monde particulier. En somme, les *botnets* de l'État islamique sont une machine qui englobe une narration humaine. Par ailleurs, il s'agit aussi d'une machine qui renvoie à de multiples fantasmes, dont celui d'une efficacité sans borne qui permettrait d'engendrer de larges cascades d'informations. Le botnet exprime en quelque sorte la promesse de l'abondance qui dépasserait les performances humaines.

Dans la réalité, les réseaux de *botnets* de l'État islamique ont uniquement déclenché des cascades de petites et de moyennes tailles. Les cascades que nous avons analysées ne dépassaient pas les milliers de *tweets* et de *retweet*. Elles n'ont par exemple jamais atteint la capacité des *botnets* russes. Dans le cas des *botnets* russes, Twitter a indiqué que plus de 50 000 *botnets* liés à la Russie ont été identifiés lors des campagnes électorales américaines de 2016 (Kantrowitz, 2018). Selon Facebook, plus ou moins 29 millions de personnes ont reçu du contenu dans le fil d'actualité provenant directement des 80 000 publications de l'Internet Research Agency[85] (Braun, 2017). Pour imager ce propos, partons d'une campagne de diffusion menée à partir d'un bloc de *tweets* préfabriqués. Le bloc contenait sept *tweets* dont la fonction était de diffuser trois communiqués de l'agence de presse A'maq concernant différentes opérations militaires menées à Damas. Ces trois communiqués ont été assemblés au sein d'une seule image, permettant une multi-latérisation de l'information. En totalisant le nombre de *tweets* et de *retweets*, les trois communiqués de l'agence de presse A'maq auront

[85] L'Internet Research Agency est une entreprise russe qui a été enregistrée en 2013 et a rapidement été connue sous le nom d'« usine à *trolls* », employant des agents rémunérés et des processus automatisés pour orienter les conversations en ligne (Benkler et al., 2018).

été diffusés 94 fois. Pour mener cette action, 54 comptes automatisés ont été déployés. Il s'agissait pour la plupart de faux comptes. Seul un des *botnets* était un compte Twitter piraté comptant 876 abonnés. D'autres cascades se soldaient quant à elle par un échec, en ne dépassant pas la dizaine de *tweets* et de *retweets*.

S'il est commun de présenter les *botnets* comme des acteurs puissants, nos résultats suggèrent qu'il faut se dégager de toute fétichisation de la machine. Tous les *botnets* ne se valent pas et il est difficile de savoir l'influence réelle qu'ils peuvent avoir sur les internautes. Ils ne forment pas un bloc unitaire qui agirait de la même manière, ils ordonnent au contraire une « individualité » (Simondon, 1958) qu'il est nécessaire d'analyser singulièrement. Ce qui singularise un botnet découle de son contexte technico-social dans lequel il s'inscrit. Si les *botnets* russes ont opéré à large échelle, c'est entre autres parce qu'ils disposaient d'une infrastructure puissante telle que l'IRA, avec des professionnels et une main-d'œuvre extrêmement efficace.

Nous ne voudrions toutefois pas donner l'illusion au lecteur d'une position normative qui se contenterait de juger ce qu'est un botnet efficace ou non. Au contraire, il faut déplacer le regard d'une anthropologie de l'homme à une anthropologie des objets techniques (Dodier, 1995), en ce que la machine consolide des manières particulières de faire de la politique. Il est vrai que le perfectionnement des robots a rendu plus aisé, moins pénible et plus rapide le pouvoir de propagation des contenus. Parallèlement, il renvoie l'humain à être un imparfait qui manque de rapidité dans sa capacité à diffuser simultanément une masse de contenus. Malgré cette incomplétude, les *botnets* n'ont pas pour autant remplacé le travail humain dans la propagation du matériel médiatique de l'État islamique. Dans la quête de rendements croissants, nous avons pu voir que les forces humaines et non-humaines s'unissaient pour améliorer le travail de diffusion.

Si tous ces changements sont d'ordre quantitatif en apparence, il n'en demeure pas moins que, comme Winner (1980) l'indiquait dans sa formule maintenant largement répandue, « artifacts have politics ». Comme nous l'avons souligné, les *botnets* sont la promesse d'une abondance et du surpassement des capacités humaines. Il ne s'agit pas seulement de simple outil amplificateur, ces arrangements de codes consolident aussi une image de la politique qui se veut technicisée et qui simule l'abondance. Il s'agit pour ces voix artificielles de créer un faux soutien ou un faux sentiment de consensus sur une idéologie particulière. Rappelons toutefois

que ces caractéristiques ne sont pas du seul apanage des *botnets*. Nous avons souligné à plusieurs reprises la manière dont les militants manipulent la plateforme pour amplifier leurs contenus. Il peut s'agir d'utiliser plusieurs comptes, de publier plusieurs fois des contenus ou des *hashtags* identiques ou encore d'interagir systématiquement avec les mêmes *tweets*. Toutes ces méthodes ont la même vocation : créer des engagements truqués. La nature même de l'œuvre de l'abondance devient par ce fait celle de la duperie et de la manipulation. Elle résulte de la capacité stratégique de la machine + de l'humain. En cela, c'est le collectif hybride qui permet la réalisation de ce programme d'action. À terme, c'est la nature même du processus dialogique qui est susceptible d'être atteint. L'objectif devenant de faire taire les hypothèses adverses et annihiler toute possibilité d'explorer le Multiple.

6.3. La guerre de l'amplification : Machine contre Machine

Le 25 avril 2017, un groupe pro État islamique sur Telegram, qui compte 243 membres, est victime d'une attaque de *spam* de la part de chiites. Cette attaque consiste à faire déferler à toute allure un flot d'images pro chiite et anti-État islamique. La même attaque se déroule simultanément contre un autre groupe pro État islamique. Un *spammeur* ressort, le botnet SEGAZOR155. Certains membres des groupes pro État islamique réagissent. Les chiites sont ciblés et il faut exclure les *spammers*. Avant que quiconque n'ait réussi à l'exclure, le botnet SEGAZOR1555 relance son attaque en actionnant la fonctionnalité /start.

> 14 : 38 Tap
> I dont get
> The shia spam here
>
> 14 : 38 SEGAZOR155
> `/start`
>
> 14 :38 Tap
> Rafida are the stupidest of people
>
> 14 : 41 Lone lion 3
> Signalez moi les spammers pour récupérer les identifiants Telegram

Ce type d'intrusion n'est pas isolé et nous avons été témoin de plusieurs attaques *spam* au cours de notre enquête. Cela résulte entre autres d'un effet d'architecture technique qui permet d'actionner facilement des *botnets*. Si nous ne pouvons établir avec certitude les auteurs de ce type d'action, nous pouvons néanmoins dire qu'elles sont majoritairement

l'objet de campagne de protestation de la part de groupes chiites. Ces attaques consistent pour l'essentiel à créer des *botnets*, à leur donner une fonctionnalité et à les connecter à un stock d'images. Cette configuration permet au *botnet* de publier à vive allure une panoplie d'images pro chiites et anti-État islamique. En somme, pour l'auteur de l'attaque, il ne s'agit pas de devoir développer de hautes compétences techniques. Comme nous l'avons déjà souligné, Telegram permet de créer facilement des *botnets*. Ainsi, il lui faudra un minimum de savoir-faire technique et d'imagination pour mener à bien son projet.

En orchestrant leur contestation autour d'un déferlement de *spam*, nous pouvons dire que ces actions représentent un mode d'action politique exercé dans le but de contraindre l'adversaire en paralysant momentanément son narratif. Ces adversaires s'en prennent aux groupes Telegram pro État islamique pour attaquer et déstabiliser leur système de représentation un bref instant. Les chiites cherchent ouvertement à attirer l'attention, il ne s'agit pas de mener des attaques dans le silence, mais de signifier leur présence à leur adversaire, de faire changer le contenu de main. Telegram devient alors un lieu de tension, où se reflète à nouveau le conflit entre chiite et sunnite : les différents groupes s'y expriment, mais cette fois-ci, sous formes iconographiques, où parole et argumentation sont absentes de l'échange. C'est ainsi à travers un langage visuel que l'auteur de l'attaque « parle ». Dans ce que nous pourrions appeler cette « logorrhée picturale », c'est-à-dire une surproduction iconographique caractérisée par un flux d'images rapides et diffuses, la plateforme numérique devient un théâtre de perturbation où se combinent interventions techniques, performances et dramaturgie.

Les images diffusées traduisent un engagement social, religieux et politique. Si nous ne pouvons être exhaustifs quant aux divers registres mobilisés, puisque la rapidité de l'action dépassait toute capacité d'observation et de capture, nous avons néanmoins pu observer quelques lignes conductrices. On trouvait par exemple régulièrement des portraits de leaders de différentes milices chiites, comme le général Qassem Soleimani, ou des martyres du Hezbollah libanais au sein de photomontages. Ces images exaltent ses combattants et leur détermination. En parallèle circulaient des emblèmes comme le drapeau iranien qui défilait de nombreuses fois lors du script joué par le *botnet* ou encore l'emblème du Corps des Gardiens de la révolution islamique[86]. Étaient également mis à l'honneur plusieurs lieux cultes de l'islam chiite : la mosquée de l'Imam Hussein (Irak), le mausolée de l'imam Reza (Iran). Le

[86] Il s'agit d'une organisation paramilitaire de la République islamique d'Iran répondant directement au Guide de la révolution, l'actuel ayatollah Ali Khamenei.

portrait de l'ayatollah Ali Khamenei apparaissait quant à lui de manière récurrente dans les différentes attaques dont nous avons été témoins. Ces images étaient d'une extrême simplicité, leur but était avant tout de témoigner et de politiser l'espace.

Toutefois, cette logorrhée picturale dépasse le cadre du simple témoignage, elle cherche également à exacerber les tensions avec ses adversaires en ridiculisant et humiliant son chef mort Abu Bakr Al-Baghdadi et ses soldats. Souvent, il s'agit d'effectuer un découpage grossier de la tête d'Abu Bakr Al-Baghdadi et de la coller dans différents photomontages. Ainsi, on pouvait voir la tête d'Abu Bakr Al-Baghdadi rattaché à différents types de corps comme celui d'un porc, d'un chien que Netanyahou et John Kerry caressent ou encore d'un homme en train de se faire décapiter. D'autres procédés de détournement consistent à remplacer son visage ou celui de ses soldats par celui d'animaux ou de l'apposer sur un corps d'âne. Une image particulièrement dégradante pour l'adversaire. Voici un exemple qui illustre une nouvelle fois la manière dont le code et les personnes deviennent solidaires dans leur lutte. Sans le *botnet*, l'objectif de perturber le réseau viendrait à s'effondrer ou du moins il serait détourné vers d'autres moyens sans doute plus lents et moins efficaces. Les adversaires ne pourraient atteindre une telle capacité d'intrusion. Le foyer d'insurrection se joue sur les plateformes. La division fratricide est traduite en matière informatique.

Pour l'État islamique, victime de l'attaque, il lui faut réaligner les acteurs. L'attaque qui manie agilité et rapidité paralyse les traductions à venir. L'issue du combat, qui ne sera jamais définitivement gagné, dépend ainsi des acteurs en présence. Comme le questionnait Callon « comment une traduction parvient-elle à résister aux assauts répétés et obstinés de traductions concurrentes, finissant par les éliminer sans qu'aucun retour en arrière soit possible ? » (1991 : 219). Les solutions offertes par l'État islamique sont doubles : l'exclusion de l'objet intrus et la robustesse de la contre-attaque. C'est dans un parallélisme des moyens, c'est-à-dire une contre-attaque iconographique, que l'État islamique constitue sa lutte (voir figure 6.12). L'intermédiaire de la lutte est tout comme son opposant le *botnet*. Le *botnet* se lance alors dans la même ronde répétitive d'images visant cette fois-ci à diffuser une série d'images menaçantes (par exemple décapitations, exécutions avec armes à feu), de conquêtes (par exemple drapeau de l'État islamique en haut de la tour Eiffel), et qui restaure l'image puissante de l'État islamique et de son ancien calife (par exemple photo de son élocution à la mosquée de Mossoul en 2014).

Tout comme son adversaire, parallèlement au fait de rappeler leur puissance, ils utilisent la

satire pour les ridiculiser, produisant un cadrage comique de leur antagoniste politique. Ils réalisent des montages simplistes et souvent de mauvaise qualité qui visent à ridiculiser le chiisme et ses ayatollahs ou encore à accuser l'Iran d'entretenir des liens avec Israël, les faisant passer pour traîtres. À travers Photoshop ou d'autres logiciels de retouche photo, cette « trahison » a été traduite de manière humoristique en réalisant différents collages, comme en témoigne la figure 6.13.

Il s'agit donc d'une manière supplémentaire de participer à la politique, ou du moins, de la continuer par d'autres moyens (Latour, 1991a). Le combat est encodé dans le dispositif. Traduire les conflits politiques en code et en pixel permet d'exploiter l'humour sarcastique d'internet, mais aussi de signaler sa puissance à son adversaire. Les classifications se font autour de personnalités, de héros, de lieux cultes et de combattants. Le public concerné est l'adversaire, qui est quant à lui amené à réagir au sein de ce que l'on pourrait appeler suivant Latour (2006b) un « *iconoclash* ».

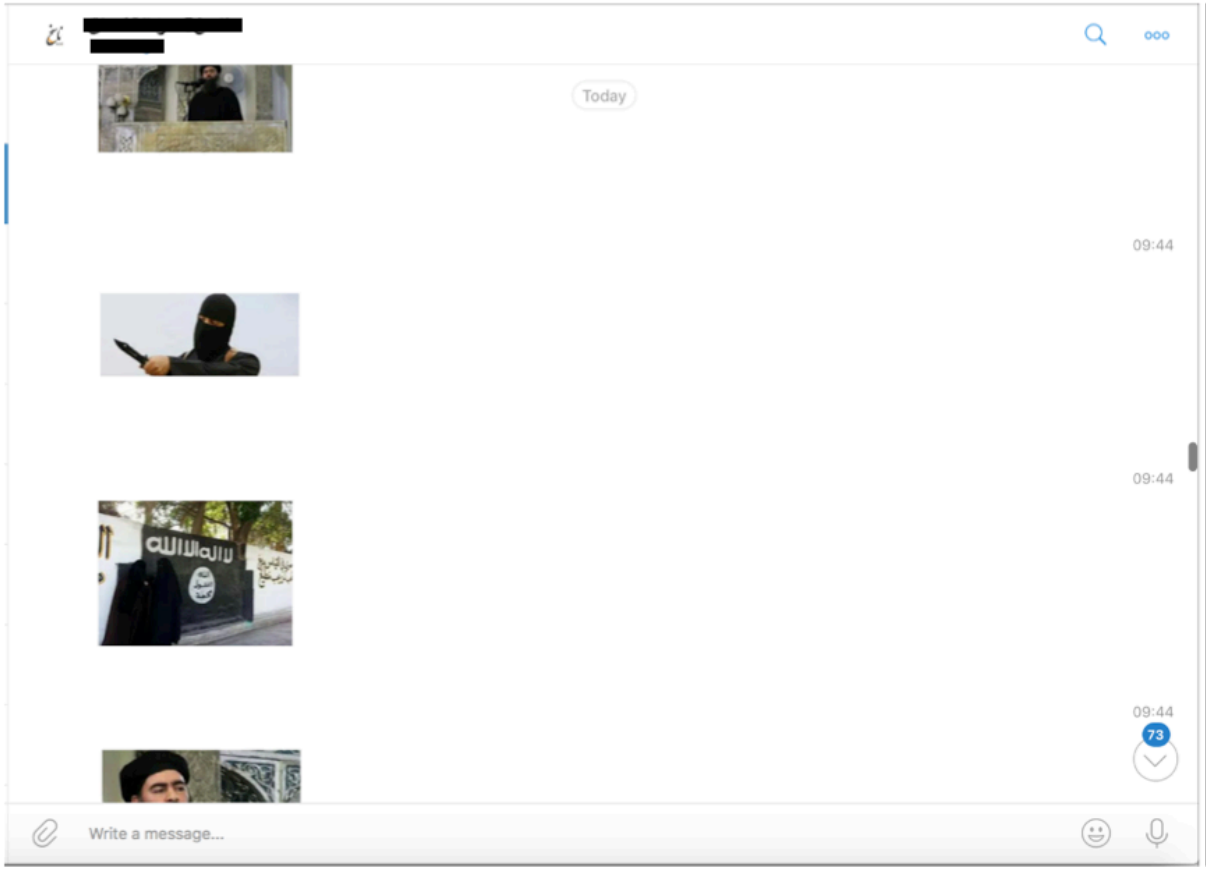

Figure 6.12. Capture d'écran du 20 novembre 2017 d'un défilement d'images pro-État islamique lors d'une attaque *spam* à l'encontre de ses adversaires. On voit se dérouler l'un à la suite de l'autre Abu Bakr Al-Baghdadi faisant son allocution à la mosquée de Mossoul en 2014, un soldat de l'État islamique pointant son couteau, un mur où on voit peint le drapeau utilisé par l'État islamique et deux femmes habillées en Burqa se promenant dans une rue qui semble paisible et calme. Le script fait réapparaître Abu Bakr Al-Baghdadi lors de son allocution à la mosquée de Mossoul, cette fois-ci sous un angle

différent.

Figure 6.12. Exemple de mèmes qui cherchent à lier le chiisme au judaïsme. Il consiste à juxtaposer à l'ayatollah Sistani et l'ayatollah Khomeini, une croix de David. Pour renforcer l'idée de bêtise, l'âne de Shrek a été ajouté au montage. Pour continuer la chaîne d'association Iran-juifs-trahison-bêtise, l'âne tient entre ses dents le drapeau de l'Iran et autour de son coup lui est joint l'étoile de David. Cette image a été diffusée lors d'une attaque spam en novembre 2017.

Conclusion : Visibilité et abondance

Ce chapitre s'est proposé d'explorer les mécanismes par lesquels le collectif jihadiste capte l'attention de ses partisans et de ses adversaires. Pour ce faire, nous avons montré comment cet objectif s'inscrit dans un programme d'amplification et d'abondance des flux infortionnels. Nous avons mis de l'avant l'ensemble des opérations tactiques et automatisées qui participent à l'amplification des énoncés sur le web. Le collectif a su profiter de la strate computationnelle pour fabriquer et distribuer ses publications. Il a démontré ses capacités à créer des contenus dans des formats qui valorisent la viralité ou, du moins, dont le sens est immédiat. Ces contenus sont environnés par la performance d'une composition machinique et humaine, informatique et culturelle. Comme l'indiquaient déjà Deleuze et Guattari (1980), « les agencements collectifs d'énonciation fonctionnent en effet directement dans les agencements machiniques, et l'on ne peut établir de coupure radicale entre les régimes des signes et leurs objets » (p.13). Par ailleurs, le collectif a optimalisé l'usage des réseaux sociaux et de ses *affordances*, en cherchant à manipuler ses algorithmes et ses fonctionnalités

informatiques. Une manipulation utile pour matérialiser le déplacement des énoncés et créer de fausses amplifications, généralement limitées au travail machinique de clic. En somme, ils ont appris à « playing the visibility game » (Cotter, 2019) sur les réseaux sociaux. Ce jeu peut être mené par des utilisateurs ou des *botnets* et nécessite dans certains cas une coordination d'envergure entre différentes plateformes numériques.

À ce stade, qu'est-ce que nos résultats nous disent sur ces mécanismes d'amplification ? Premièrement, ces processus s'apparentent à une rationalisation opérationnelle qui requiert que les machines et les humains soient solidaires entre eux. L'ordonnance d'un modèle guidé par les promesses de l'abondance repose en effet sur l'efficacité des humains et des non-humains à s'associer et à se stabiliser, de la quantité des êtres mobilisés, de la performance de ces agencements et de leur capacité à assurer la fabrication et la diffusion des énoncés. Ainsi, chacune des étapes de conception, de production et de distribution implique un « potentiel d'activité » (Boltanksi et Thévenot, 1987) qui repose sur l'enrôlement de puissantes forces. Ces forces humaines et non-humaines s'affirment dans leur différence et dans leur association. Les mécanismes de production et de distribution mettent dès lors en œuvre de l'énergie, du mouvement, des machines et des méthodes.

Deuxièmement, nos résultats illustrent la façon dont le collectif organise l'espace avec de nouveaux aménagements, des redéfinitions et des détournements. En d'autres termes, l'action d'abondance et d'accumulation menée par des humains ou des non-humains n'est possible que dans un environnement de comportements nuisibles qui valorisent le *spam*, le *trolling*, le harcèlement et la duperie. Pour amplifier leur message, les partisans détournent des *hashtags* de manière abusive, profèrent des hostilités à l'encontre d'utilisateurs, personnalités publiques et agences de presse et fabriquent de fausses amplifications. Cela peut parfois créer une tension entre les utilisateurs qui s'échangent des insultes et des menaces les uns envers l'autre.

Troisièmement, leurs mécanismes d'amplification apparaissent dans l'ensemble maîtrisés, avec des opérations d'assistance et de stockage. Dans ce modèle de l'abondance, nous avons pu voir que les corps sont l'outil premier travaillant à la fabrication et à la distribution des énoncés. Ils vacillent également dans des rôles qui orchestrent des campagnes décentralisées sur Twitter à l'aide de chaînes Telegram spécialisées. Des campagnes qui, on l'a vu, sont par ailleurs peu effectuées par des militants et généralement déléguées à des *botnets*. Quant à la matérialité informatique, elle n'est pour le collectif qu'un moyen de prolonger la manipulation

de l'attention. Elle forme l'équipement du jihadiste afin de matérialiser et déplacer leurs énoncés. Pour entretenir l'accumulation et la croissance, il n'existe donc pas un stratège, mais un collectif hybride qui mise sur des actions à la fois créatives et machiniques.

Enfin, cette logique d'accumulation et d'abondance mène à de nouvelles configurations et interactions. Notre dernière section montre notamment comment les guerres médiatiques ne sont plus seulement menées d'humains à humains, mais aussi de machines à machines. Les adversaires automatisent des réseaux de *botnets* qui s'affrontent dans des luttes iconographiques et énonciatives. Dans ces combats automatisés, on retrouve un ensemble d'énonciations qui mêlent la grandeur et la puissance du groupe, l'humiliation de l'adversaire ainsi que l'humour sarcastique d'internet.

Chapitre 7 : La modération, un frein au travail de diffusion

Jusqu'à présent, nous avons mis en relief les premières opérations de traduction entre les plateformes numériques et les militants de l'État islamique. On pouvait percevoir une certaine convergence au sein de ce réseau technico-jihadiste. À ce stade, la relation était encore floue et sans limites. Pourtant, des conflits et des tensions ont rapidement émergé. De nombreuses forces opposées se sont organisées pour tenter de contrer le projet jihadiste au sein du web. Pour y voir plus clair, ce chapitre saisira les contraintes de coopération entre le dispositif technique et l'usager jihadiste. Plus précisément, il rendra compte d'un moment critique pour le collectif : le renforcement de la modération au sein des plateformes. Ce faisant, nous considérerons la modération comme un « anti-programme ». Akrich et Latour définissent les anti-programmes comme « all the programs of actions of actants that are in conflict with the programs chosen as the point of departure of the analysis; what is a program and what is an antiprogram is relative to the chosen observer » (1992 :261). Ce chapitre laissera ainsi transparaître un autre versant de l'histoire, celui de ce moment où atteindre l'objectif de visibilité devient laborieux et incertain.

Le point de vue privilégié ne sera plus seulement celui des utilisateurs jihadistes, mais celui des dispositifs engagés par l'action. Outre le matériel en ligne, nous nous baserons dans ce chapitre sur d'autres sources, telles que de la documentation produite par les firmes ou encore les déclarations des fondateurs des plateformes. Nous procéderons aussi à une analyse des internautes qui sont d'actifs participants dans la lutte contre le terrorisme en ligne. Notre démarche s'effectue en quatre temps. Après quelques précisions sur les nouvelles législations qui contraignent davantage les plateformes numériques et les utilisateurs jihadistes, la deuxième partie s'intéresse à la manière dont la modération s'organise au sein des plateformes. La troisième section aborde le vaste réseau d'acteurs nécessaire au fonctionnement de la modération. Enfin, nous terminerons en décrivant la transformation de la modération en objet de luttes, de conflits et de détournement.

7.1. Les contraintes de la coopération entre le dispositif technique et l'utilisateur

Rappelons que durant une bonne partie de son histoire, la Silicon Valley a ardemment défendu les valeurs du Premier Amendement[87] (Citron, 2018). Lorsqu'elle modérait les contenus enfreignant les termes de service, elle le faisait dans le strict respect des valeurs de la liberté d'expression américaine. Or, la diffusion en ligne de discours qualifiés d'extrémistes a placé ces firmes dans une position difficile au cours des dernières années. On dira à leurs propos qu'elles fournissent des réponses insuffisantes à la propagation des discours extrémistes. À cet égard, elles sont critiquées et accusées pour leurs politiques de sécurité trop laxistes. Quant aux gouvernements, ces derniers multiplient les tentatives d'obtenir une plus grande collaboration dans la lutte contre le terrorisme de la part des plateformes numériques. Ils attendent de celles-ci qu'elles suppriment plus agressivement les contenus extrémistes en ligne, qu'elles rendent accessibles aux autorités les conversations cryptées pour faciliter la surveillance, et qu'elles améliorent la coopération judiciaire [88].

Parmi tant de débats et de critiques, c'est l'image des plateformes numériques qui se dégradent. Le risque absolu pour celles-ci est de voir leur valeur commerciale se détériorer. C'est ainsi que face aux multiples pressions et à un cadre législatif plus sévère, les plateformes numériques se sont mises à revoir leurs politiques en matière de liberté d'expression et ont commencé à abriter un ensemble de tactiques pour lutter contre les discours extrémistes. Dans les prochaines sections, nous mettrons l'accent sur plusieurs moments clés de la réorganisation du dispositif technique pour qu'il modère plus efficacement les contenus extrémistes.

7.1.1. Un nouveau cadre juridique pour l'utilisateur et l'objet technique

Aux États-Unis, la section 230 de la Communication Decency Act de 1996 accorde aux plateformes numériques une large immunité à propos de ce que ses utilisateurs publient. En les délivrant du statut d'éditeur, cette loi leur permet d'établir leurs propres normes en matière

[87] Le Premier amendement des États-Unis vise à garantir la liberté d'expression, en interdisant au Congrès d'adopter des lois qui la limiteraient.

[88] Prenons le cas du plan d'action pour lutter contre le terrorisme sur internet mis en place en juin 2017 par le président français Emanuel Macron et de l'ancienne Première ministre britannique Theresa May. Ce plan d'action comprend quatre axes de travail : la mise en place d'une censure a priori ; permettre l'accès au contenu chiffré à des fins d'investigation ; accélérer l'accès aux données et aux contenus stockés aux États-Unis ; soutenir et promouvoir le contre-discours.

de contenu. Comme le note Gillespie (2018), sa particularité est qu'elle agit à un double niveau : si la loi n'oblige pas les plateformes à surveiller ce que ses utilisateurs publient, elle protège en même temps celles qui décident de supprimer des contenus en ligne. Somme toute, la loi défend tant les plateformes qui ne font rien en matière de régulation de contenus, que celles qui ont un rôle plus actif dans la suppression et le contrôle des contenus illicites. Cet acte législatif forme ce que l'auteur appelle une « double immunité ».

En août 2015, un juge californien a par exemple rejeté la plainte des familles de deux Américains tués dans une attaque revendiquée par l'État islamique en Jordanie[89]. Les plaignants accusaient le réseau Twitter d'avoir fourni un « soutien matériel » à l'État islamique et de lui servir d'instrument de propagande. En fondant sa décision sur la Communication Decency Act, le juge a considéré que les plateformes en ligne n'étaient pas responsables du contenu publié par les utilisateurs. Il n'en demeure pas moins que les gouvernements de plusieurs démocraties libérales ont exercé d'importantes pressions auprès des acteurs de la Silicon Valley pour qu'ils renforcent leur dispositif de régulation des contenus.

Lors de notre enquête, nous avons été témoins de renforcements toujours plus sévères concernant le filtrage de contenus en ligne. L'intervention des gouvernements dans la régulation du réseau s'est cependant effectuée à différents niveaux. Les États-Unis ont par exemple favorisé la voie du partenariat avec les plateformes des médias sociaux, tout en les incitant à être plus proactives en matière de lutte contre les contenus terroristes. À l'inverse, les gouvernements européens ont plus souvent mis en place de nouvelles législations en matière de régulation de contenus illicites. Au demeurant, il est de coutume que les États-Unis interviennent minimalement au sein du réseau et plus spécifiquement en matière de régulation des contenus, en raison du Premier Amendement. Les dernières années en Europe ont quant à elles été le théâtre de l'expansion de mécanismes législatifs contraignant les utilisateurs et les plateformes numériques.

L'exemple de la France

La France, pays emblématique en matière de renforcement des dispositions relatives à la lutte contre le terrorisme, a depuis 2014 institué plusieurs dispositifs qui ciblent directement

[89] À propos de ce cas : https://www.lapresse.ca/international/dossiers/le-groupe-etat-islamique/201608/10/01-5009323-rejet-dune-plainte-accusant-twitter-de-disseminer-le-message-de-lei.php

internet et les comportements en ligne[90]. On observe un renforcement des peines en cas d'apologie ou de provocation du terrorisme lorsque les faits ont été commis en ligne. Pendant un bref délai, la consultation habituelle d'un service de communication en ligne qui met à disposition des contenus incitant directement à la commission d'acte terroriste ou en faisant l'apologie était punissable d'une peine d'emprisonnement[91]. Cet arrêté a néanmoins été jugé inconstitutionnel en 2017.

Les nouvelles dispositions donnent aussi plus de pouvoir aux autorités administratives, en leur accordant l'autorisation de faire du blocage administratif de sites web terroristes, ainsi que de déréférencer des sites provocants à des actes terroristes. Ces lois ont fait l'objet de critiques permanentes et diversifiées de la part des défenseurs du web. Les critiques s'articulent essentiellement autour du fait que le contournement des institutions judiciaires porte atteinte au principe de séparation de pouvoirs et comporte un risque de blocage disproportionné. Ces mesures démontrent aussi une conception plutôt naïve de la technologie. Effectivement, le blocage peut être facilement contournable en utilisant par exemple le réseau TOR ou des services de proxy. De plus, il est possible que les sites visés réapparaissent avec de nouvelles adresses ou qu'ils soient hébergés hors de la France. Enfin, ils s'appliquent seulement à des sites web dans leur intégralité et non à des pages spécifiques d'un site donné. Cela signifie que le dispositif est totalement inopérant pour les réseaux sociaux, puisque le blocage d'un nom de domaine ne permet pas de cibler une page Facebook ou un compte Twitter individuel.

Contraindre les plateformes numériques

Nous avons également observé l'apparition d'un autre type de dispositif législatif qui ne vise cette fois-ci non plus à incriminer les comportements en ligne, mais à tenir juridiquement responsables les plateformes des réseaux sociaux de ce que leurs utilisateurs publient en ligne. Nous renvoyons cette pratique à ce que MacKinnon qualifie de « *intermediary liability*» puisque « the *intermediaries*, or companies transmitting or hosting users' communications or other content, are held *liable* for their users' and coustomers' behavior » (2012 :93).

Au sein des pays européens, c'est l'Allemagne qui a été la plus agressive avec la loi *Netzwerkdurchsetzungsgesetz* (ou plus simplement appelée NetzDG ou Network Enforcement

[90] Voir à ce propos la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme :
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029754374&categorieLien=id
[91] Une exception était faite, si la consultation était effectuée de « bonne foi ».

Act) entrée en vigueur le 1er octobre 2017. Si cette loi touche les contenus terroristes et anticonstitutionnels, elle s'inscrit dans les débats plus larges de régulation de contenus en matière de discours haineux et de désinformation. La loi NetzDG somme les plateformes numériques qui comptent plus de deux millions d'utilisateurs inscrits en Allemagne de mettre en place une procédure de traitement des demandes de suppression de contenu qui soit à la fois efficace, rapide et transparente. La loi prévoit par exemple l'obligation pour les plateformes de réseaux sociaux qui reçoivent plus de 100 plaintes au cours d'une année civile de fournir un rapport trimestriel sur leurs efforts entrepris en matière de traitement des contenus illicites. Les plateformes doivent aussi prévoir une procédure de signalement facilement reconnaissable et directement accessible pour les utilisateurs.

Enfin, et c'est surtout sur ce dernier point que la loi a fait débat, il est exigé des compagnies des réseaux sociaux qu'elles suppriment ou bloquent l'accès à un contenu « manifestement illicite » endéans les 24 heures suivant la réception de la plainte. Dans le cas où l'illégalité du contenu n'est pas manifeste, la loi prévoit un délai de sept jours suivant la réception de la plainte pour supprimer ou bloquer immédiatement l'accès au contenu. Face au non-respect de ces nouvelles règles, les plateformes numériques sont passibles d'une amende pouvant aller jusqu'à 50 millions d'euros, même si l'infraction n'est pas commise en Allemagne.

Aujourd'hui, nous constatons le développement d'initiatives qui généralisent de telles réglementations. Dans la même veine, la Commission européenne a proposé en 2018 un règlement « relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne ». Le règlement s'étend dans ce cas-ci à tous les acteurs du web et ne vise plus seulement les grandes plateformes des médias sociaux. Il prévoit que les plateformes web bloquent ou suppriment le contenu dans un délai d'une heure à compter de la réception de l'injonction de suppression émise par une décision administrative ou judiciaire d'un État membre. Il impose également aux plateformes de prendre des mesures proactives en ce qui concerne la suppression des contenus terroristes, par le déploiement d'outils de détections automatisés.

Ainsi que nous le montre cet aperçu, la plupart des mouvements institutionnels formels et législatifs délèguent la modération de contenus terroristes aux entreprises des plateformes numériques. Nous aimerions apporter une nuance ici. En réalité, comme l'a montré notre chapitre 2, la modération a toujours fait partie des plateformes numériques et les pouvoirs publics se sont toujours immiscés, d'une manière ou d'une autre, dans le contrôle de l'information. On peut penser par exemple aux pays autoritaires qui utilisent le filtrage et le

contrôle pour brimer la liberté d'expression sur internet ou encore l'obligation pour les plateformes numériques de se conformer à certaines lois locales de différents pays.

Néanmoins, les nouvelles lois que nous avons présentées ci-dessus amènent une nouvelle donne : les plateformes numériques sont davantage contraintes de prendre le rôle de *gatekeepers*, parfois dans un temps imparti. Les gouvernements placent ainsi la frontière de la régulation des contenus plus loin que ne l'auraient souhaité les représentants des plateformes numériques. Pour Twitter, il s'agit de « menaces juridiques à la liberté d'expression ». À cet égard, nous pouvions lire sur un billet posté sur leur *blog* :

> With the passage of new legislation and ongoing regulatory discussions taking place around the world about the future of public discourse online, we are seeing a potential chilling effect with regards to freedom of expression. According to Human Rights Watch, the wave of regulatory pressure in Europe and beyond is setting an emerging precedent and creating a "domino effect" as "governments around the world increasingly look to restrict online speech by forcing social media companies to act as their censors."[92]

Ces nouveaux mécanismes punitifs ne sont pas sans effet. Premièrement, ils risquent de placer les plateformes dans une posture de prudence extrême. En ce sens, pour éviter les amendes, elles pourraient adopter des définitions plus larges et censurer ainsi des contenus licites. Les rapports de transparence diffusés à ce jour par les compagnies montrent toutefois que la plupart des contenus supprimés ont été faits en vertu du règlement de la communauté, plutôt que d'une disposition légale locale comme la loi NetzDG[93]. Deuxièmement, ces législations imposent aux plateformes d'instaurer des dispositifs qui demandent des ressources technologiques, économiques et humaines considérables. En l'état, seuls les géants du web sont actuellement en mesure de se conformer à de telles obligations. Peut-être faudrait-il y voir à terme le risque d'une monopolisation de la modération par les géants du web.

[92] Extrait du communiqué *Expanding and building #TwitterTransparency*, Twitter, 5 avril 2018

[93] Voir par exemple le rapport de transparence YouTube sur la suppression de contenu en vertu de la loi NetzDG : https://transparencyreport.google.com/netzdg/youtube?hl=fr&community_guidelines_enforcement=period:Y2019H1&lu=community_guidelines_enforcement. Notons que jusqu'en janvier 2019, seule la catégorie « contenu terroriste ou anticonstitutionnel » contenait plus de suppression en vertu de la loi NetzDG que selon les standards de la communauté. Une différence qui peut s'expliquer par le fait que les définitions du terrorisme diffèrent d'un contexte politique à l'autre, rendant par conséquent difficile pour les plateformes de déterminer ce qu'est un contenu terroriste ou non. Toutefois, au cours de ces derniers mois, cette tendance s'est inversée : plus de contenus terroristes ont été supprimés en raison du non-respect du règlement de la communauté.

7.2. Refuser le rôle « d'hébergeur de contenus »

Nous avons vu tout au long de la description précédente que les dispositifs techniques sont maintenant pris dans un tissu de contraintes et de législations. Ces nouvelles exigences opèrent sur les plateformes numériques une prise immédiate : elles exigent que le dispositif technique devienne un agent du contrôle social. Ces contraintes sont liées à une logique de sécurisation de l'espace qui force les plateformes numériques à refuser leur rôle d'hébergeur de contenu dans des circonstances particulières. L'exercice du contrôle se manifeste par la mise en place d'un « dispositif de sécurité » qui ne vise plus à soumettre, commander, discipliner, normaliser l'individu, mais bien à en assurer la « bonne » gestion des flux en excluant les éléments nuisibles (Foucault, 1978).

Le paradigme de la sécurité se pose non plus en termes de clôture pour protéger un territoire national, mais en termes de contrôle des passages. Cette posture entre en résonnance avec l'analyse remarquable qu'avait donnée autrefois Foucault sur la transformation des villes et leur administration au XVIIIe siècle. À cette époque en effet, la suppression des murailles a altéré les capacités de surveillance des allées et venues. Cela a eu pour conséquence d'accroître l'insécurité des villes face à l'afflux de toutes les populations « flottantes » – mendiants, délinquants, criminels – en provenance, entre autres, de la campagne. Il est dès lors devenu crucial d'organiser la circulation en écartant ceux qui étaient perçus dangereux. S'en est suivi une dichotomie entre la bonne et la mauvaise circulation : « Il s'agit simplement de maximaliser les éléments positifs, que l'on circule le mieux possible, et de minimiser au contraire ce qui est risque et inconvénient comme le vol, les maladies, tout en sachant parfaitement qu'on ne les supprimera jamais » (Foucault, 1978 : 21). De la même façon, aujourd'hui, pour canaliser la fluidité des flux informationnels, les plateformes trient, sélectionnent et filtrent les éléments nuisibles à la circulation.

Pour assurer la bonne gestion des flux, les plateformes numériques doivent renoncer à leur rôle d'hébergeur de contenus que les militants de l'État islamique lui attribuent. En refusant ce rôle, les plateformes numériques cherchent à rompre leur relation avec l'internaute indésirable. La coordination entre le dispositif et son utilisateur se ternit inéluctablement. Elle devient périlleuse, voire impossible. Ce flux problématique est venu chambouler le dispositif technique qui doit maintenant développer des stratégies propres à l'exclusion de ce type particulier d'utilisateur. Le terme de stratégie est ici propice, parce que « le résultat du

fabricant est le résultat d'un calcul et d'une réflexion sur ses moyens d'action » (Thévenot, 1993 : 100-101).

Dans ce cas, la mise en place de stratégies dépend de la mobilisation d'un réseau d'actants, comprenant les entreprises, des ingénieurs, des algorithmes, des utilisateurs, des experts en terrorisme, etc., juxtaposé par plusieurs modalités de coordinations, dont la fonctionnalité de signalement, l'apprentissage automatique ou encore les Règles et Politiques de la communauté. Nous arguons que le degré de coordination s'exécute au travers d'une série de procédures qui consistent à catégoriser, créer un dispositif d'intéressement et trouver des alliés. Cette « mise en plan » d'un filtrage puissant est l'occasion de montrer qu'il agit à partir de procédures extrêmement opaques, technico-centrées et asymétriques.

7.2.1. Inscrire l'usager dans la posture du « mauvais utilisateur »

Pour développer une stratégie efficace, le dispositif technique doit d'abord cibler l'utilisateur problématique. On entre dans des opérations élémentaires de catégorisation. Avec cette action, le dispositif technique est en mesure d'inscrire l'utilisateur dans une nouvelle posture : celle d'un « mauvais utilisateur » et plus spécifiquement, d'un « utilisateur terroriste ». Cette nouvelle posture ménage une série de dispositifs techniques et sociaux pour qu'elle fonctionne (Akrich, 2006). Il faut l'inscrire dans une nouvelle chaîne de traduction qui est celle de « l'exclusion-du-mauvais-utilisateur ». Ce déplacement a fait émerger de nouveaux savoirs et une foule de rôles inédits dans l'exercice de la sécurité.

En vue d'interdire des pratiques qui font voir l'objet technique sous un mauvais jour, les injonctions sont souvent présentes dans les « Règles et Politiques » associées aux plateformes numériques[94]. À défaut d'avoir un cadre juridique entourant les plateformes, elles ont eu recours à la mise en place de règles et règlements qui sont souvent à la base du contrôle social (Benkler et al., 2018). Les règlements sont supposés indiquer à l'utilisateur d'une plateforme en ligne les usages autorisés ou non. Ils introduisent les degrés de liberté et dictent la manière de se comporter. Ces règles sont en constantes évolutions et chacune des plateformes se réserve le droit d'effectuer des modifications.

Aussi banal soit-il, le règlement est une pièce importante du dispositif technique qui ordonne

[94] De la même manière, Akrich et Boullier (1991) démontrent l'importance du « mode d'emploi » pour signaler à l'utilisateur la manière dont il doit s'emparer de l'objet technique. Le mode d'emploi est pour les auteurs « la mise en scène d'un rapport didactique » (p.114).

et pose les termes des usages sous la forme d'un « contrat » entre l'objet technique et l'utilisateur. Pour ainsi dire, il est destiné à sanctionner les mésusages et à assurer un contrôle sur le flux informationnel. Ce contrat passé entre l'objet technique et l'utilisateur est unilatéral, sans négociation possible : l'utilisateur choisit de s'y conformer ou non.

> Nous pensons que tout le monde devrait avoir l'opportunité de créer et de partager instantanément des idées et des informations, sans aucun obstacle. Pour protéger l'expérience et la sécurité des utilisateurs de Twitter, nous avons défini certaines restrictions qui s'appliquent au type de contenu et au comportement autorisés. Ces restrictions sont énoncées ci-dessous dans les Règles de Twitter.
>
> Les Règles de Twitter (ainsi que toutes les politiques qu'elles regroupent), notre Politique de confidentialité et nos Conditions d'utilisation constituent le « Contrat d'utilisation de Twitter », qui régit l'accès d'un utilisateur aux services de Twitter et à l'utilisation de ceux-ci[95].

Les plateformes font prévaloir l'idée que la communication entre les internautes ne peut s'effectuer que dans le seul cadre d'un lieu sécuritaire. Dans le cas contraire, la liberté d'expression et l'interaction ne s'exerceraient pas confortablement. La valeur du contrat réserve le droit au dispositif technique d'exercer des sanctions en cas de non-respects, montrant par ce biais son caractère opérationnel. Il est l'élément clé pour justifier la fin de la coopération entre le dispositif et l'usager. Les sanctions peuvent aller d'un bannissement partiel à un bannissement total.

> Toutes les personnes qui accèdent aux services de Twitter ou les utilisent doivent se conformer aux politiques énoncées dans les Règles de Twitter. En cas de non-respect, Twitter pourra prendre l'une ou plusieurs des sanctions suivantes[96] :

- exiger que vous supprimiez le contenu interdit pour pouvoir de nouveau créer des publications et interagir avec les autres utilisateurs de Twitter.
- limiter temporairement votre capacité à créer des publications ou à interagir avec les autres utilisateurs de Twitter.
- vous demander de vérifier la propriété du compte avec un numéro de téléphone ou une adresse mail.
- suspendre définitivement votre compte ou vos comptes.

C'est dans un style simple et accessible à tous que les plateformes inscrivent la posture du « mauvais utilisateur ». Cela prend la forme de brefs paragraphes, sections, listes, visuels. Ces règlements rendent explicite à l'usager son programme d'action, ce qui est attendu de lui. Par

[95] Préambule des Règles de Twitter en date du 17 avril 2019
[96] Liste des sanctions prises par Twitter en cas de non-respect de ses règles en date du 17 avril 2019

ailleurs, ils l'obligent à se délier de la plateforme dans le cas où il prendrait la posture d'« utilisateur terroriste ». Ce pouvoir de la règle ne signifie pas pour autant que les injonctions sont respectées. Au contraire, les plateformes luttent continuellement face aux internautes jihadistes qui reviennent à la suite de suspensions. Si les règlements exercent un certain pouvoir qui dirige l'opération, l'utilisateur a quant à lui son propre registre d'action pour défier l'objet technique, comme nous le verrons dans le chapitre suivant.

En vue d'effectuer une démarcation entre le « bon utilisateur » et le « mauvais utilisateur », les dispositifs techniques utilisent des catégories évocatrices qui reconduisent et renforcent les images de violence et de dangerosité associées au terrorisme. C'est sous les rubriques de type « organisations et individus dangereux », « violence », « violence et blessures » des sites des plateformes des médias sociaux que nous aurons accès à ce type de posture.

> Violence et blessures :
> Violence : il est interdit d'exprimer des menaces de violence spécifiques ou de souhaiter la mort, la maladie ou des blessures physiques à une personne ou à un groupe de personnes. Cela inclut, sans toutefois s'y limiter, les menaces de terrorisme ou l'apologie de celui-ci. Par ailleurs, vous ne devez pas vous associer à des organisations qui par leurs propres déclarations ou activités sur la plateforme comme en dehors, utilisent la violence à l'encontre de civils pour servir leur cause, ou incitent à la violence à cette fin[97].

En gardant un flou sur ce que Twitter entend par « terrorisme », la plateforme de réseaux sociaux nous heurte à un problème de taille. Comment assurer un processus de transparence et de responsabilité de la part du dispositif technique quand la posture n'est pas définie ? Parmi les plateformes des réseaux sociaux, seul Facebook fournit une définition de ce qu'il considère comme terroriste.

> Nous n'autorisons pas les individus (vivants ou décédés) et groupes suivants à maintenir une présence (par exemple, en possédant un compte, une Page, un groupe) sur notre plateforme[98] :
>
> Les organisations terroristes et les terroristes
>
> - Une organisation terroriste correspond à :
> - Toute organisation non gouvernementale impliquée dans des actes de violence prémédités contre des individus ou une propriété en vue d'intimider une population civile, un gouvernement ou un organisme international et avec pour objectif d'atteindre un but politique, religieux ou idéologique

[97] Règles Twitter en matière de contenus violents en date du 17 avril 2019
[98] Définition du terrorisme par Facebook dans ses Standards de la Communauté en date du 17 avril 2019

- Un membre d'une organisation terroriste et toute personne commettant un acte terroriste sont considérés comme des terroristes
    - Un acte terroriste correspond à tout acte de violence prémédité contre des individus ou une propriété, perpétré par une personne n'appartenant pas à un gouvernement en vue d'intimider une population civile, un gouvernement ou un organisme international, avec pour objectif d'atteindre un but politique, religieux ou idéologique.

Cette définition large renvoie au sens commun du terrorisme contemporain qui se comprend comme : « des actes de violence exécutés par des groupes politiques généralement clandestins, dans la volonté de créer un climat d'insécurité, d'affaiblir un régime, de désorganiser un système d'oppression visant tant les individus que les biens » (Sorel, 2002 : 37). Elle offre ainsi une grande latitude pour classifier des phénomènes qui entrent dans cette catégorie générale. De ce fait, être terroriste dépend du point de vue de celui qui le définit (Bigo, 2005). Il est impossible de savoir à ce stade qui Facebook considère comme terroriste. Ce n'est qu'en consultant les documents de l'entreprise et les rapports de transparence que nous verrons qu'il associe la propagande terroriste uniquement aux groupes jihadistes tels que l'État islamique et Al-Qaïda.

Ce faisant, les plateformes sont extrêmement sélectives dans le choix des groupes terroristes qu'elles décident de bannir. En réduisant le terrorisme à des groupes jihadistes, la plateforme renforce les mythes qui entourent l'islam et le terrorisme. En ce sens, les formes de sélection opérées par le dispositif technique contribuent à structurer une conscience commune sur le terrorisme. Maintenant que nous avons vu comment les plateformes numériques catégorisent un « mauvais utilisateur », il nous reste à voir la manière dont ces catégorisations deviennent opérationnelles. Pour ce faire, le dispositif technique devra constituer une nouvelle chaîne de traductions qui permet de passer de la catégorisation à celles de dispositifs proactifs.

7.2.2. La fonction de signalement comme dispositif d'intéressement

Pour que les injonctions soient respectées, les dispositifs techniques ont mis à disposition une fonctionnalité informatique qui permettra d'atteindre l'objectif de modération. Chaque plateforme a son propre dispositif de signalement et se réserve le droit de le modifier à tout instant. Certains signalements ciblent le contenu directement ; tandis que d'autres permettent de signaler un compte, une chaîne, une page ou un profil. Si ces outils ont subi une évolution constante au sein des différentes plateformes, la tendance actuelle des grandes plateformes

numériques est d'offrir un dispositif de signalement facilement reconnaissable et directement accessible pour les utilisateurs qui souhaitent signaler un contenu illégal.

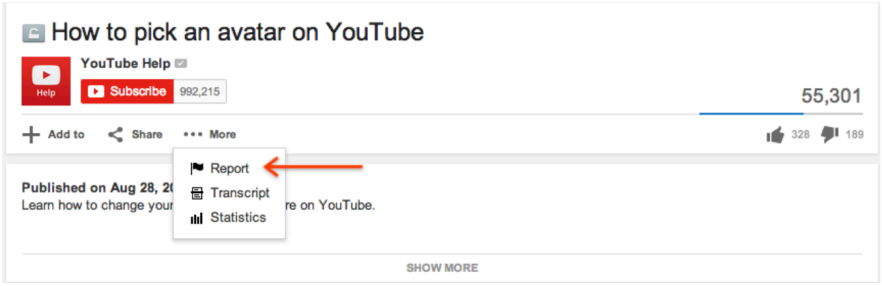

Figure 7.1. Interface YouTube de la rubrique « comment signaler une vidéo », capture d'écran datant du 18 avril 2019.

Le dispositif de signalement lie ainsi le dispositif technique à tout internaute qui a l'intention de faire appliquer une norme. Cette zone de collaboration se matérialise donc par un dispositif technique simple, un outil de signalement. Celui-ci traduit l'application d'une norme, en un bouton, qui retraduit lui-même, la variété des comportements proscrits, et qui transforme en bout de compte l'actant en agent du contrôle social. Généralement, il ne suffit pas pour l'internaute de simplement signaler le contenu ou le profil problématique. Afin de donner une valeur opératoire au signalement, il faut que l'internaute justifie son choix à partir d'une liste proposée par la plateforme. Le nombre d'éléments compris au sein de la liste et les catégories varient d'une plateforme à l'autre. Des plateformes comme Twitter et Telegram ne font par exemple jamais mention de terrorisme, mais de contenus « violents », de « propos dangereux et inappropriés » ou d'images « sensibles », au contraire de Facebook et YouTube qui proposent les catégories de « terrorisme » ou d'« incitation au terrorisme ». Il s'agit d'une brève procédure pour que la plateforme comprenne la raison du signalement, et en même temps, puisse entraîner ses algorithmes d'apprentissage automatique.

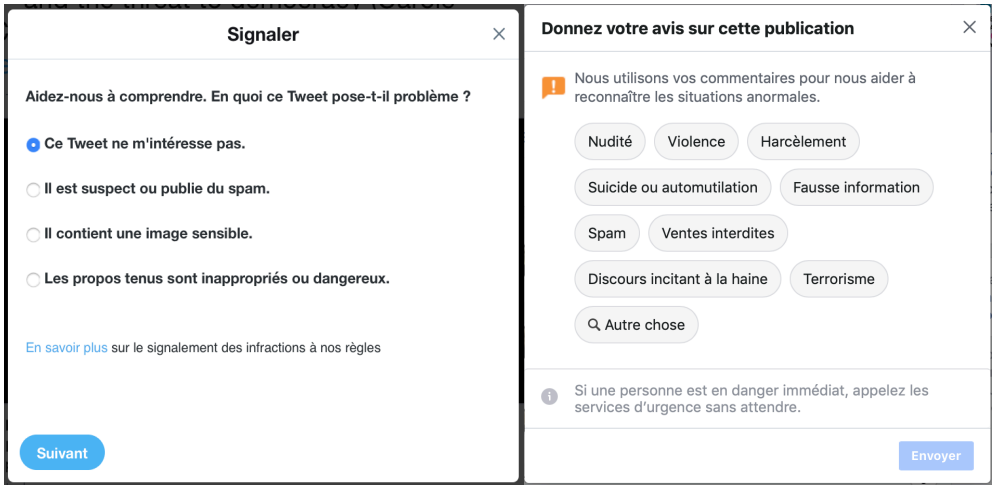

Figure 7.2. Fenêtre de signalement Twitter à gauche, fenêtre de signalement Facebook à droite en date du 10 avril 2019.

Dans l'exemple ci-dessus, on peut également voir que Facebook ajoute une responsabilité morale de plus à ses utilisateurs, en l'incitant à appeler les services d'urgence dans les cas où une personne est en danger immédiat. Cette incitation amène davantage de responsabilités auprès de l'utilisateur qui est cette fois-ci mis à contribution pour garantir la sécurité des autres internautes. Ces mécanismes démontrent que la relation entre l'hébergeur et l'internaute n'est plus considérée comme une simple relation de service. La plateforme inscrit ici l'utilisateur dans une « communauté » à protéger et elle lui attribue un rôle dans la régulation des flux informationnels.

Ce rôle est toutefois limité, puisqu'en fin de compte les plateformes se réservent le droit de modérer ou non le contenu. À la suite du signalement, la plateforme se sert de tous les niveaux de l'opacité bureaucratique et technique pour dissimuler l'arrière-scène de la modération. Une fois le signalement opéré, il devient une boîte noire. Les équipes de modération, réparties aux quatre coins du monde pour assurer une modération en continu, exercent leur rôle dans le secret le plus total. Les plateformes dévoilent peu d'informations sur ses équipes de modération, à qui elles la sous-traitent et la manière dont elles opèrent pour décider du sort d'un contenu. Le dispositif technique met ainsi en relation une série d'actants, parfois totalement invisibles les uns pour les autres. Il n'est pas question de systèmes de négociation ou d'espaces délibératifs, plus que d'un ensemble d'étapes succinctes et routinières où chaque élément du système a un rôle attribué et mécanisé (du clic de signalement au clic de suspension).

Notons que si la fonction de signalement peut être comprise comme un « dispositif d'intéressement », cela n'assure en rien le succès. Suivant Callon, « aucun dispositif de capture aussi contraignant soit-il, aucune argumentation aussi "convaincante" soit-elle, n'est assuré de succès » (1986 : 189). Ce n'est pas parce que la fonction est là qu'il y a forcément enrôlement. Si l'un des principaux coups de ruse des plateformes est d'avoir mis en place des systèmes de signalement facile à utiliser, il n'empêche que ce n'est pas tous les utilisateurs qui se sentiront concernés par cette « responsabilité morale » qui lui est déléguée. Pour que la chaîne de traduction fonctionne, il faudra que le dispositif technique trouve des alliés de taille. Il sera alors question d'enrôler à la fois des humains et des non-humains.

7.3. À la recherche d'alliés

Les plateformes numériques « n'exposent » pas, « ne figurent » pas, « n'objectivent » pas un dispositif de sécurité. Elles les constituent et les organisent. Toutefois, les plateformes ne parviennent pas à construire une sécurité solidement établie par la coercition textuelle, des notices, des avertissements. C'est pourquoi il leur faut déployer le réseau de leurs relations, construire des alliances, recruter des équipes d'ingénieurs, des experts, des modérateurs, et mobiliser leurs utilisateurs ainsi que les mathématiques et ses principes de code. La relative stabilité de ce réseau abrite tout un jeu de subtiles coordinations et négociations qui permet à la modération de fonctionner. Plus spécifiquement, l'engagement à modérer les « mauvais flux » repose sur trois piliers : l'utilisation de systèmes d'apprentissage automatiques, le recours à l'expertise humaine et le renforcement de collaborations.

Dans ce qui suit, nous décrirons ces modalités de coordination. En nous inspirant de Callon (1986), nous distinguerons des coordinations « locales » et « générales ». La coordination à portée locale, concerne l'ensemble des dispositifs découlant directement de l'entreprise et qui nécessite un travail de mise en œuvre par cette dernière (les algorithmes d'apprentissage automatique), quant à la coordination à portée générale elle concerne toute la communauté interne ou externe à la plateforme (les utilisateurs, les gouvernements, les ONG, etc).

7.3.1. L'algorithme comme coordination à portée locale

Au-delà des injonctions inscrites dans les Règles et Politiques des compagnies, ces dernières disposent de moyens supplémentaires pour en assurer le maintien et le respect. C'est parce que le contrôle ne peut se construire uniquement avec des humains et parce que les Règles et Politiques laissent encore trop de liberté qu'il faut des algorithmes. Dès lors, la plupart des compagnies de réseaux sociaux ont mis en place des pratiques de retrait automatisées et semi-automatisées. Depuis quelques années, les acteurs privés et publics conçoivent que l'art d'exclure les contenus terroristes doit se pratiquer au travers de la technologie et plus précisément au sein d'outils d'intelligence artificielle. On pouvait notamment lire dans un communiqué de Mark Zuckerberg publié sur Facebook :

> Artificial intelligence can help provide a better approach. We are researching systems that can look at photos and videos to flag content our team should review. This is still very early in development, but we have started to have it look at some content, and it already generates about one-third of all reports to the team that reviews content for our community. It will take many years to fully develop these systems. Right now, we're starting to explore ways to use AI to

> tell the difference between news stories about terrorism and actual terrorist propaganda so we can quickly remove anyone trying to use our services to recruit for a terrorist organization. This is technically difficult as it requires building AI that can read and understand news, but we need to work on this to help fight terrorism worldwide[99].

Bien que les compagnies des géants du web reconnaissent qu'elles en sont encore à leur balbutiement, elles promettent que la technologie, et plus spécifiquement l'intelligence artificielle, deviendra plus puissante dans les années à venir pour assurer la protection et la sécurité d'internet. Les plateformes espèrent plus particulièrement une amélioration en ce qui concerne les capacités de l'intelligence artificielle à distinguer les nuances linguistiques.

Une telle équivoque apparaît clairement dans ce qu'il est commun de désigner un « solutionnisme technologique ». Morozov (2014) a amplement explicité la poussée de la fétichisation du solutionnisme technologique au sein des acteurs de la Silicon Valley. Pour faire bref, il s'agit de propager l'idée que les technologies innovantes apporteraient des solutions rapides et efficaces à tous les problèmes épineux. À ce titre, les compagnies des médias sociaux ont eu tendance à présenter leurs algorithmes de détection automatique comme une sorte de « kit solutionniste » qui suppriment les contenus rapidement, à grande échelle et souvent avant même qu'ils soient visualisés par un internaute. On peut à partir de là voir que l'algorithme est entièrement conçu pour avoir l'avantage sur les flux en circulation.

> By using technology like machine learning, artifical intelligence and computer vision, we can proactively detect more bad actors and take action more quickly.[100]

Actuellement, ces technologies de détection reposent principalement sur des algorithmes d'apprentissage automatique. Les instructions ne sont plus programmées explicitement par un ingénieur, mais sont générées par la machine elle-même qui apprend sur base des données qui lui sont fournies (Burrell, 2016). L'auteur rappelle que cette procédure a pour conséquence de rendre la logique sous-jacente de l'algorithme totalement incompréhensible et opaque pour tout observateur, ainsi que pour ses concepteurs. L'algorithme lui-même ne « comprend pas » ce qu'il fait, il agit uniquement sur une masse de données à partir desquelles il établit des prédictions. Pour modérer les contenus, les algorithmes reposent principalement sur deux types de mécanismes.

Le premier est celui de la « correspondance d'images ». Pour supprimer des vidéos ou des

[99] Extrait du communiqué « *Building Global Community »*, Mark Zuckerberg, 16 février 2017
[100] Extrait du communiqué « *Removing Bad Actors From Facebook »,* Facebook, 26 juin 2018

photos, les plateformes utilisent la technologie dite « d'empreinte numérique » (« *hash* »). Cette technologie consiste à attribuer une empreinte à un fichier. C'est ainsi que lorsqu'un utilisateur télécharge une nouvelle vidéo ou image terroriste, le système vérifie si l'image correspond à une photo ou une vidéo terroriste connue. Si le système trouve une correspondance, le contenu est bloqué pratiquement instantanément. Deuxièmement, les plateformes ont particulièrement investi dans la compréhension linguiste, en expérimentant l'utilisation de l'intelligence artificielle pour comprendre un texte qui pourrait préconiser de la propagande terroriste. Ces algorithmes apprennent entre autres à détecter des publications terroristes à partir de textes de propagande terroriste d'Al-Qaïda et de l'État islamique déjà supprimés. Si ces technologies en sont encore à leur premier stade, les algorithmes d'apprentissage automatique fonctionnent sur une boucle de rétroaction, qui lui garantiront une amélioration au cours du temps.

En outre, pour maximiser le potentiel de détection des comptes jihadistes, le contenu ne constitue pas le seul indicateur utilisé par les plateformes numériques. Un autre moyen est d'utiliser des algorithmes qui détectent des « grappes terroristes », c'est-à-dire que par exemple Facebook (2017) se sert de « signals like whether an account is friends with a high number of accounts that have been disabled for terrorism, or whether an account shares the same attributes as a disabled account ». Par ailleurs, le dispositif technique s'associe également à des algorithmes qui repèrent les « comptes récidivistes ». Ce terme qui fait directement référence à un langage criminologique concerne les internautes frauduleux qui recréent de faux comptes à la suite de leur suspension. Ainsi, nous pouvions lire :

> Recidivism: We've also gotten much faster at detecting new fake accounts created by repeat offenders. Through this work,net we've been able to dramatically reduce the time period that terrorist recidivist accounts are on Facebook. This work is never finished because it is adversarial, and the terrorists are continuously evolving their methods too. We're constantly identifying new ways that terrorist actors try to circumvent our systems — and we update our tactics accordingly[101].

En résumé, l'intervention algorithmique est multiple et intervient sur différents niveaux ; celui du profil, des contenus, des relations ou encore des usages. L'idéal associé à ces algorithmes est de permettre une coercition ininterrompue qui réduirait l'occurrence et l'impact des flux problématiques. Cette conception ressemble étrangement à de nombreux travaux en criminologie (Feeley et Simon, 1992 ; Slingeneyer, 2007) qui ont montré qu'au sein de la

[101] Extrait du communiqué « *Hard Questions : How We Counter Terrorism* », Facebook, 15 juin 2017

« nouvelle pénologie », le crime était abordé comme un risque normal, un problème technique. Dans ce cas, le crime est un accident. Il s'agit d'un risque « dont il faut essayer de prévoir l'occurrence et minimiser les impacts négatifs » (Slingeneyer, 2007 : 3). L'enjeu devient de réguler les niveaux de déviances et de pouvoir anticiper le crime de façon à y répondre de manière préventive. La réponse technique apportée à la régulation des flux illicites s'inscrit dans ce même paradigme d'un risque « normal » et « quotidien » dont il faut réduire l'apparition et en retarder la survenue.

La règle morale traduite dans un langage informatique se transforme ainsi en une suite d'instructions que l'algorithme doit exécuter. Or, comme le stipule John Dewey, « la morale n'est pas un catalogue d'actes ou un ensemble de règles à appliquer comme une ordonnance ou une recette de crise » (2014 : 226). Au contraire, les règles morales ne constituent pas une fin en soi, mais doivent être mises à l'épreuve, elles ont besoin de méthodes spécifiques d'enquête et de bricolage. En tant qu'instrument, sa valeur réside dans sa capacité de travail, c'est-à-dire sa capacité à être testée et confirmée en fonction des conséquences provoquées par les pratiques. Or, dans le cas de l'algorithme, il n'est pas question de débat, puisque de par sa vision totalisante, il donne l'illusion de voir juste. Sa seule contrainte : avancer toujours plus rapidement et plus efficacement.

Une loupe puissante

Comme nous l'avons déjà stipulé, pour qu'un algorithme fonctionne, il lui faut des données. En ayant une vision globale des internautes, c'est-à-dire de ses communications, de ses actions à la fois visibles et silencieuses, l'algorithme agit comme une loupe puissante qui permet de catégoriser certains utilisateurs et contenus comme terroristes. Ces « empreintes numériques » apparaissent constitutives d'un « comportementalisme radical » (Cardon, 2015) dès lors qu'elles établissent des ensembles de relations entre des comportements passés. L'algorithme ne se base pas seulement sur l'historique d'activités de l'utilisateur, il opère également un travail sur les traces numériques de ceux qui ont effectué les mêmes actions que lui. Ce mécanisme est qualifié plus généralement dans le jargon technique de « filtrage collaboratif ». La prédiction de l'algorithme repose donc également sur « le passé de ceux qui lui ressemblent » (Cardon, 2015 : 34).

Le fait d'être catégorisé comme terroriste découle ainsi d'un ensemble de signaux. Ce pouvoir d'énonciation n'appartient plus seulement à des instances gouvernementales ou officielles,

mais est le fait d'une agrégation de données provenant d'entreprises privées (Cheney-Lippold, 2018). En catégorisant l'individu à partir d'un ensemble de traces numériques, l'algorithme exerce un pouvoir de narration sur l'individu. Cheney-Lippold le résume extrêmement bien « we are narratized when our data is algorithmically spoken for » (2018 :39). Dans le cas des algorithmes de détection, ces derniers « disent » quelque chose en langage mathématique à propos de l'utilisateur, il lui assigne une posture d'utilisateur légitime ou illégitime. En cela, le dispositif algorithmique retraduit dans une prétendue objectivité les catégorisations construites au sein des Règles et Politiques des plateformes, à partir de données « brutes » qui « historicisent » l'utilisateur. Ces opérations de catégorisation montrent que finalement le dispositif technique est un outil puissant qui condense la mise au passé et le présent de l'utilisateur.

Ce pouvoir algorithmique de connaissance sur les internautes est d'autant plus renforcé lorsque les géants du web décident de s'allier et de mettre en commun leur base de données, comme en témoigne le Global Internet Forum to Counter Terrorism (GIFCT). Il s'agit d'un partenariat créé en 2017 entre Facebook, Microsoft, Twitter et YouTube. Ce partenariat a pour but de nuire à la capacité des terroristes de diffuser leurs contenus, en développant des moyens technologiques efficaces et en partageant les meilleures pratiques. La puissance de ce partenariat s'articule dans leur base de données commune créée en décembre 2016. Elle vise à partager des « *hachages* » (ou « empreintes ») d'images et de vidéos terroristes pour en arrêter la propagation. Au terme de plusieurs années de collaboration, le GIFCT vante « l'efficacité accrue » de cette collaboration, avec une base de données qui renferme plus de 100 000 « *hashes* ».

> By sharing these hashes with one another, we can identify potential terrorist images and videos on our respective hosted consumer platforms. This collaboration is resulting in increased efficiency as we continue to enforce our policies to help curb the pressing global issue of terrorist content online.
>
> As part of the GIFCT, the founding companies committed to refine and improve the shared industry hash database, and we have made important progress over the past year:
>
> - The database now contains more than 100,000 hashes. It allows member companies to use those hashes to identify and remove matching content – videos and images – that violate our respective policies or, in some cases, block terrorist content before it is even posted.
> - The Hash Sharing Consortium includes Ask.fm, Cloudinary, Facebook, Google, Instagram, Justpaste.it,

> LinkedIn, Microsoft, Oath, Reddit, Snap, Twitter and Yellow. We will work to add to new members throughout the upcoming year.[102]

Face à ce savoir global et à une capacité d'analyse à grande échelle, l'algorithme informatique se voit attribuer une capacité normative supérieurement légitime, car lui seul peut rapporter les « signaux terroristes » et trouver la voie d'action la plus rationnelle. Qui plus est, ce pouvoir s'exerce essentiellement au sein des géants du web qui ont le monopole sur des bases de données colossales, nécessaires à la consolidation et au fonctionnement de leurs algorithmes d'apprentissage automatique. Dans les discours des entreprises technologiques, il n'est par ailleurs jamais question des potentiels biais que le traitement de ces données pourrait reproduire ni de système d'audits qui évalueraient l'algorithme. Les algorithmes opèrent dans la plus grande opacité. Pour les compagnies technologiques, les algorithmes ont une « disposition à l'objectivité » (Hillis et al. 2013 : 37) et sont désintéressés, politiquement parlant. Il témoigne d'un destin rationnel à son apogée, qui évince le fait qu'il soit une « opinion intégrée dans les mathématiques » (O'Neil, 2016).

Publiciser le « succès » par les chiffres

Si, comme nous venons de le voir, l'algorithme travaille dans le plus grand des secrets, il est appelé à quitter la clandestinité pour afficher ses succès au sein de rapports de transparence de plus en plus exigés par les gouvernements. L'analyse de ces rapports permet de dresser un constat sans équivoque : les algorithmes signalent plus de contenus que les êtres humains. Depuis l'intégration des techniques automatisées, les entreprises suppriment plus de contenus et plus rapidement et elles trouvent la majorité des contenus elles-mêmes. Concernant les contenus terroristes, les résultats obtenus à ce jour grâce au progrès des techniques automatisées montrent un taux de succès de plus de 90 %[103] :

- YouTube : 98 % des vidéos supprimées par YouTube pour extrémisme violent sont signalées par des algorithmes d'apprentissage automatique. Actuellement, l'apprentissage automatique permet de supprimer cinq fois plus de vidéos qu'auparavant.

- Twitter : Entre janvier 2018 et juin 2018, 205 156 comptes au total ont été définitivement suspendus pour des infractions liées à la promotion du terrorisme.

[102] Résultats du partenariat diffusé sur le site du GIFCT.
[103] Ces résultats proviennent des rapports de transparence des plateformes.

Parmi ces suspensions, 91 % étaient des comptes signalés de manière proactive par des outils internes.

- Facebook : 99.7 % du contenu terroriste lié à l'État islamique et à Al-Qaïda qui a été supprimé sur Facebook l'a été avant que quiconque de la communauté ne le signale et, dans certains cas, avant qu'il ne soit diffusé sur le site. Une fois que Facebook est au courant d'un contenu terroriste, 83 % des copies téléchargées ultérieurement sont supprimées dans l'heure qui suit.

Toujours dans le but de convaincre de sa puissance d'action et, surtout de ses capacités d'évolution, les entreprises ont tendance à communiquer les progrès spectaculaires que leurs algorithmes ont effectués depuis leur récente introduction.

> For example, at the beginning of 2017, 8 percent of the videos flagged and removed for violent extremism were taken down with fewer than 10 views. We introduced machine learning flagging in June 2017. Now more than half of the videos we remove for violent extremism have fewer than 10 views[104].

Si un effort de transparence peut être constaté au sein des entreprises, il n'est par ailleurs en rien synonyme de responsabilité. Ces chiffres, difficilement vérifiables, posent certains problèmes. Pour commencer, comme l'indique Facebook, les chiffres qui sont rattachés à la prédominance des violations concernant la propagande terroriste ne peuvent être estimés de manière fiable. De plus, étant donné que les variables qui font fonctionner l'algorithme et leurs bases de données ne sont pas connues, il est difficile de vérifier ce qui est catégorisé comme terrorisme et les potentiels biais. Enfin, les entreprises parlent rarement des faiblesses de leurs algorithmes et pour ainsi dire jamais de leur taux d'erreurs[105]. Elle dédommage ainsi l'algorithme d'une question centrale : Et s'il se trompait ? Plusieurs commentaires s'imposent sur ce point. Lors de nos observations sur Twitter, nous avons été témoins à plusieurs reprises de ce type de *tweet* :

> Hey @Twitter, can you please unsuspend @Adam_Bachaa ? He is a terrorism analyst, not a terrorist. (Twitter, 10 avril 2019).

[104] Extrait du communiqué « *More information, faster removals, more people – an update on what we're doing to enforce YouTube's Community Guidelines* », YouTube, 23 avril 2018

[105] Depuis 2019, Facebook publie toutefois dans son rapport de transparence les contenus qui ont été restaurés après appel ou non. Par exemple, en ce qui concerne les contenus supprimés pour motif de terrorisme, entre janvier et mars 2019 : 157 300 contenus ont été restaurés sans appel et 20 100 ont été restaurés avec appel (sur les 48 600 appels effectués). Durant cette même période, 6,7 millions de contenus ont été supprimés pour motif terroriste.

Généralement, les victimes de ces erreurs sont des veilleurs-analystes de groupes jihadistes ou de la guerre en Syrie et en Irak. Bien que nous ne puissions établir avec certitude si c'est l'humain ou l'algorithme qui est derrière cette erreur de modération, les utilisateurs ont eu tendance à pointer la responsabilité des algorithmes. Cet exemple nous permet de rebondir sur l'une des limites de l'algorithme aujourd'hui largement admises au sein des entreprises de technologie : les systèmes d'apprentissage automatique s'avèrent extrêmement mauvais pour comprendre le contexte du discours. Facebook explique dans l'un de ses communiqués que :

> AI can't catch everything. Figuring out what supports terrorism and what does not isn't always straightforward, and algorithms are not yet as good as people when it comes to understanding this kind of context. A photo of an armed man waving an ISIS flag might be propaganda or recruiting material, but could be an image in a news story. Some of the most effective criticisms of brutal groups like ISIS utilize the group's own propaganda against it. To understand more nuanced cases, we need human expertise[106].

Ainsi, au stade de développement actuel des algorithmes d'apprentissage automatique, plusieurs constats peuvent être soulignés. Premièrement, l'humain est plus compétent pour comprendre la complexité et le contexte contrairement aux algorithmes d'apprentissage automatique. S'ils aident à signaler plus rapidement un contenu douteux, on ne peut pas leur faire confiance pour le supprimer ni pour signaler une menace crédible qui mériterait d'être rapportée aux forces de l'ordre. Une délégation totale de la modération à des systèmes automatisés mènerait à des risques de censure totalement disproportionnés. Par ailleurs, la difficulté pour les développeurs est de développer une « technologie intégrative » qui fonctionne sur différents types de média. Lorsqu'un algorithme est programmé pour une séquence particulière, il dispose de peu de marge de manœuvre pour s'adapter à un autre ensemble de données.

> In figuring out what's effective, we face the challenges that any company faces in developing technology that can work across different types of media. For instance, a solution that works for photos will not necessarily help with videos or text.[107]

Pour terminer, son usage est extrêmement limité. Les compagnies expliquent qu'un système conçu pour rechercher le contenu d'un groupe terroriste ne fonctionne pas sur d'autres groupes en raison des différences de langage et de style dans la propagande. Les compagnies ont ainsi eu tendance à concentrer leur système de détection automatique sur « les groupes

[106] Extrait du communiqué « *Hard Questions: How We Counter Terrorism* », *op. cit.*
[107] *Ibid.*

terroristes qui constituent la plus grande menace au niveau mondial, dans le monde réel et en ligne » (Facebook, 2017), à savoir l'État islamique et Al-Qaïda. En cela, en ce qui concerne le terrorisme, elles ne se concentrent que sur un seul type de menace.

Machine + humain

Alors que l'algorithme est généralement présenté comme une force puissante et autonome, il lui faut pourtant des ingénieurs, des experts, des ONG, des gouvernements, la société civile, des modérateurs, etc., pour qu'il puisse fonctionner. Étonnamment, si les entreprises de technologie vantent le déploiement de leurs algorithmes de détection, elles n'ont cessé d'engager plus de personnes dans leurs équipes de sécurité et de sûreté. En 2018, Facebook a doublé le nombre de personnes travaillant au sein de ces équipes, passant à 20 000 employés, dont 7500 réviseurs de contenu. Google est passé quant à lui à 10 000 employés.

> The Value of People + Machines : Deploying machine learning actually means more people reviewing content, not fewer. Our systems rely on human review to assess whether content violates our policies[108].

Outre les ingénieurs impliqués dans leur construction, l'expertise humaine reste essentielle dans deux types de domaines. Le premier, et comme nous l'avons déjà évoqué, est de discerner le contexte du contenu. Le second est de former et entraîner les systèmes d'apprentissage automatique. Cela consiste à réviser des millions de contenus extrémistes et violents pour aider l'algorithme à identifier des contenus similaires par la suite. Ces travailleurs de l'ombre permettent aux plateformes de construire leurs algorithmes de modération et d'en assurer leur efficacité. Ce « travail du clic »[109] anonyme et précaire, capturé sous la notion de « digital labor » (Casilli, 2017, 2018 ; Cardon et Casilli, 2015), relativise la prétendue automatisation du travail de l'algorithme.

L'algorithme ne peut ainsi être assemblé en structure stable que par une opération de fabrication et d'entraînement du dispositif. Il est dépendant de l'humain tant au niveau de sa conception que lors de son fonctionnement. Comme nous venons de le voir avec

[108] Extrait du communiqué « *More information, faster removals, more people – an update on what we're doing to enforce YouTub's Community Guidelines* », *op. cit.*

[109] Ces services de « clics » achetés par les grandes plateformes numériques sont généralement sous-traités en Philippines, au Pakistan, en Inde, en Chine ou encore au Bangladesh, créant d'importants flux de « digital labor » entre des entreprises des pays occidentaux et des pays émergents et en voie de développement (Graham et al., 2017).

l'augmentation du nombre d'employés au sein des équipes de sécurité des plateformes, l'automatisation n'a ici pas tant remplacé l'humain, plus qu'elle en a multiplié son nombre. Visiblement, ce sont précisément les machines automatisées qui ont le plus besoin d'humains. À ce titre, comme le stipulait déjà Simondon en 1958 à propos des machines à auto-régulation : « tandis que les autres machines n'ont besoin de l'humain que comme servant ou organisateur, les machines à auto-régulation ont besoin de l'humain comme technicien, c'est-à-dire comme associé ; leur relation à l'humain se situe au niveau de cette régulation, non au niveau des éléments ou des ensembles » (p. 174).

Pour maximiser l'expertise, les compagnies ont par exemple engagé plus d'experts en matière d'extrémisme violent et de contre-terrorisme. Ils ont aussi augmenté leur partenariat avec d'autres sociétés de technologie, des gouvernements, des groupes de la société civile, des universitaires et ONG. L'idée qui guide ces partenariats est de favoriser un apprentissage partagé du terrorisme et des mécanismes de propagande reliés à l'État islamique et Al-Qaïda. Par exemple plusieurs organisations spécialisées dans le terrorisme ou la cybersécurité, peuvent signaler des pages, des profils et des groupes sur les plateformes. Tout comme elles peuvent envoyer aux compagnies des fichiers photos et vidéo associés à l'État islamique et Al-Qaïda, que les entreprises exécutent ensuite sur leurs algorithmes pour vérifier la correspondance de fichiers afin de supprimer ou d'empêcher leur téléchargement sur la plateforme.

Nous pouvons donc conclure que l'algorithme est un agencement d'humains et de non-humains, il est « solidaire » d'une action de contrôle, plus qu'il ne la mène de façon autonome. La modération a tant besoin de la technologie que des personnes. Afin que les exigences normatives de l'objet technique soient respectées, elles doivent donc passer par un partenariat humain-machine. La modération devient l'aboutissement d'un collectif hybride où différentes entités s'entrecroisent et échangent à la fois des propriétés et des connaissances.

7.3.2. La communauté pour une coordination à portée générale

Malgré que la plupart des signalements soient effectués à l'interne par des algorithmes, les compagnies en cause cherchent aussi à enrôler la communauté des utilisateurs dans ce processus. Ce rôle est généralement proposé dans les politiques et règles de sécurité des plateformes. On peut ainsi trouver des énoncés comme : « nous comptons sur les membres de la communauté YouTube pour signaler les contenus qui leur paraissent inappropriés » ; « nous

[Facebook] demandons aux gens de partager du contenu de manière responsable et de nous informer lorsqu'ils observent quelque chose qui peut enfreindre nos Standards de communauté ». La mise en place d'un ordre social sur les plateformes implique donc une diffusion de la responsabilité. La communauté est incitée à prendre le rôle de surveillant des flux informationnels. Par ce fait, les plateformes généralisent la fonction de surveillance à tout un chacun. Les plateformes présentent ce travail de surveillance comme totalement utile et nécessaire à son bon fonctionnement. À côté des algorithmes, l'utilisateur fait marcher son propre sens de la régulation du dispositif, en se conformant aux injonctions de la plateforme. L'utilisateur à l'esprit civique devient alors assistant du dispositif technique. Il ne dirige pas l'ordre social, mais se conforme anonymement au « travail du clic de signalement » prescrit par le dispositif.

Plus concrètement et de manière plus utilitariste, les plateformes ont essentiellement besoin de la communauté là où ses algorithmes de détection ne sont pas efficaces, c'est-à-dire pour tous les contenus qui sont en instantanés et en direct. Si les plateformes sont capables de filtrer grâce à leurs algorithmes de détection la plupart des photos et des vidéos qui ont déjà fait l'objet de suspensions (et donc contiennent une empreinte), par définition ce n'est pas le cas dans les vidéos en direct proposées par certaines plateformes. Prenons le cas de Facebook qui a introduit la vidéo en direct en 2016. En 2016, Larossi Abballa a fait usage du Facebook Live pour revendiquer le meurtre de deux fonctionnaires de police à leur domicile à Magnanville, en tournant sa vidéo sur place. La vidéo a duré 13 minutes, a été vue en direct par 98 personnes et a été retirée 11 heures après sa diffusion. Plus récemment, le Facebook Live a été activité lors de la tuerie de Christchurch. Visionnée par 4000 personnes, il a fallu 29 minutes pour que la vidéo ait son premier signalement et soit supprimée. L'algorithme a été mis hors-jeux, car confronté à des données sur lesquelles il n'a jamais pu s'entraîner (même si la compagnie a développé des technologies capables de repérer certains thèmes ou images dans des vidéos en direct et de les bloquer immédiatement[110]). Quant aux membres de la communauté, ils semblaient trouver un intérêt à visionner la vidéo.

Pour mener à bien l'ordre social sur leur plateforme, les entreprises sélectionnent également des partenaires de choix dans la fonction de signalement. Prenons l'exemple du programme « Trusted Flagger » mis en place par YouTube. Ce dernier permet de « fournir des outils puissants aux utilisateurs, aux agences gouvernementales et aux organisations non

[110] Voir à ce propos : https://www.newyorker.com/news/news-desk/inside-the-team-at-facebook-that-dealt-with-the-christchurch-shooting

gouvernementales (ONG) qui signalent avec efficacité des contenus qui enfreignent le Règlement de la communauté ». Il équipe les Trusted Flagger de différents avantages comme :

- Un outil de signalements groupés permettant de signaler plusieurs vidéos à la fois
- Un forum d'assistance privé pour toute question relative à la procédure de mise en application des règles
- Des informations sur les décisions prises pour les contenus signalés
- L'examen prioritaire des contenus signalés pour une plus grande efficacité

Les « Trusted Flagger » sont sélectionnés par YouTube. Le critère de sélection est le suivant : signaler régulièrement des contenus avec un taux de fiabilité élevé. Les compétences du « Trusted Flagger » sont évaluées continuellement et à tout moment. YouTube se réserve le droit de retirer le statut dans les cas où le « Trusted Flagger » signalerait régulièrement des contenus qui n'enfreignent pas le règlement de la communauté la plateforme. Dans les taux de signalement, les Trusted Flagger arrivent en deuxième position loin derrière les algorithmes[111].

Ce qui est préoccupant avec ce type de programme est qu'il sélectionne des agences gouvernementales qui seront en mesure d'exercer un droit de censure avec des moyens privilégiés. Ainsi faut-il rappeler les valeurs des pionniers d'internet, celles des politiques de dérégulations et de valeurs libertaires (Cardon, 2010). Or, depuis qu'internet s'est rempli d'intermédiaires privatisés, les instances gouvernementales ont davantage de prise pour contrôler l'information en ligne. Nous avons déjà vu dans le chapitre 2 comment certaines entreprises technologiques cherchent à satisfaire les demandes gouvernementales pour accéder à des marchés économiques. Nous avons aussi vu dans ce chapitre, comment l'activité législative dans le secteur de l'information a gravi de nouvelles étapes. Maintenant, nous pouvons voir comment certains géants du web fournissent des outils à des autorités gouvernementales pour signaler des contenus jugés problématiques. Ces mécanismes qui banalisent le contournement de la justice et portent atteinte à la séparation des pouvoirs se prévalent dans la plus grande opacité. À l'heure actuelle, nous ne savons pas quelles sont les agences gouvernementales sélectionnées, selon quels motifs et les types de contenus qu'elles signalent majoritairement.

[111] Pour le trimestre d'octobre 2018 à décembre 2018, les contenus détectés automatiquement étaient de 6 190 148 contre 1 942 913 pour les Trusted Flagger.

7.4. Le monde de la dénonciation

Comme nous l'avons souligné, les compagnies comptent sur leurs utilisateurs pour signaler tout comportement inapproprié. Est-ce pour autant que certains utilisateurs endosseront ce rôle ? Très certainement. Et qui plus est, avec une implication extrêmement active. Nos observations quotidiennes nous ont fait naviguer à travers un océan d'internautes qui ont pour principale mission de dénoncer des comptes jihadistes. Ces internautes sont en quelque sorte l'incarnation de l'enrôlement réussi pour multiplier les signalements de contenu délétère. Mais, ces actions ne sont pas univoques : elles mènent à un climat de revanche, à des affrontements et à d'innombrables disputes entre les communautés adverses. Nous verrons tout au long de cette section comment la fonction de signalement fait l'objet de conflits et de luttes stratégiques.

7.4.1. Les cyber-vigilants et la dénonciation : un enrôlement réussi

Face à la recrudescence des contenus jihadistes et des attentats en occident, certains utilisateurs et collectifs d'hacktivistes, comme Anonymous [112] se sont attribués la responsabilité et le devoir moral de dénoncer auprès des compagnies les comptes terroristes. Il n'est pas possible de cerner avec exactitude le moment où la mobilisation d'Anonymous et d'autres hacktivistes a commencé. On sait toutefois qu'en 2015, à la suite des attentats menés contre Charlie Hebdo[113], Anonymous a affirmé sa volonté de riposter contre des sites qualifiés d'islamistes, ainsi que des comptes de réseaux sociaux appartenant à des extrémistes présumés[114]. Ces « utilisateurs justiciers » s'érigent en quelque sorte en porte-parole de la lutte anti-terroriste en ligne. Ils mettent en œuvre des actions pour que le dispositif technique « change de main » et que son affectation soit revue (Boltanski, 1990). Le message de ces internautes est clair : il ne peut être utilisé pour des motifs de propagande terroriste. Pour que l'objet technique retrouve sa stabilité, ces utilisateurs utilisent des moyens discursifs et techniques pour combattre et éliminer les utilisateurs indésirables.

Cette action ne résulte d'aucun pacte formel, aucune récompense en cas de dénonciation, aucune punition en cas de non-dénonciation. Elle reflète plutôt une initiative citoyenne qui

[112] Anonymous est un collectif apparu en 2007, son combat fondateur est celui du maintien de l'anonymat et de la libre circulation de l'information. Au-delà, Gabriella Coleman indique que le collectif ne défend ni philosophie, ni programme politique cohérent : « Bien que le collectif soit reconnu pour sa contestation dans l'univers numérique et ses actions directes, il n'a jamais affiché d'orientation claire » (2016 :11).
[113] Les attentats contre Charlie Hebdo se sont déroulés le 7 janvier 2015 à Paris et ont été revendiqué par Al-Qaïda dans la péninsule arabique (AQPA).
[114] Voir à ce propos « Les Anonymous contre l'État islamique » : http://www.slate.fr/story/110691/anonymous-contre-daech.

estime avoir le devoir moral de s'engager dans la lutte anti-terroriste en ligne. L'action ne se réduit pas à un collectif unique. Elle est le fait d'internautes individuels, dont certains se réclament d'Anonymous, et de collectifs spécialement constitués pour lutter contre la propagande jihadiste en ligne, par exemple CtrlSec ou encore le Katiba des Narvolos. D'ailleurs, pour accroître l'ampleur de leur action, ces utilisateurs tentent d'enrôler toujours plus de partisans en les convaincant qu'il s'agit d'une cause juste qui peut être facilement menée. Comme le stipule le collectif Ctrlsec : « quelques clics suffisent pour accélérer leur élimination ». Cela suit une logique simple : plus les signalements sont nombreux, plus il y a de chance que le compte en question soit suspendu.

Malgré la diversité des internautes impliqués, certaines constances peuvent être observées. Il s'agit d'une masse d'anonymes qui parle sous couvert d'une opération, celle de « Operation ISIS » traduite sous le *hashtag* #OpISIS. Les *hashtags* signifiant l'opération se sont toutefois multipliés et ont inclus des variantes telles que #OpJihad, #OpIceISIS ou encore #OpDaesh. La mission parcourue par ces « armées d'internautes » est par exemple clairement énoncée dans la biographie du profil Twitter de CtrlSec qui ne compte pas moins de 25 800 abonnés :

> Our mission is to limit and destroy online extremism in all shapes. To participate in the cause please report the targets sent from our accounts.

Ce passage est révélateur des objectifs et actions entreprises par ces utilisateurs et collectifs : détruire la présence en ligne de l'État islamique en signalant leurs comptes auprès des compagnies. Ces internautes ne prennent pas la plume en leur nom propre, mais aiment se présenter comme des « traqueurs » et des « chasseurs » qui poursuivent les comptes des jihadistes.

> Thanks to all amazing hunters and to all those who support us while we helping @Twitter to be a better place. #OpISIS #Ar_OpIceISIS (Twitter, 23 mars 2017)

Le fait qu'il parle au nom d'une action autorise l'internaute à utiliser un ensemble de codes partagés entre eux, comme des *hashtags* spécifiques à l'opération, la mise en scène de la dénonciation, des images parodiques ou encore des images de mise en preuve. Lorsque ces internautes décrivent par exemple leurs opérations, ils ont tendance à utiliser un vocabulaire qui privilégie l'ordre de grandeur de leur mouvement. Les Kaliba des Narvalos parlent d'une « initiative inédite sur les réseaux sociaux ». Sur un autre profil Twitter publiant une image du masque de Guy Fawkes, on pouvait lire le message suivant :

> OPERATION ISIS HAS BECOME THE LARGEST ENDEAVOR IN THE HISTORY OF ANONYMOUS. UNITED TOGHETER AS ONE WE CAN CHANGE HISTORY. ANONYMOUS (Twitter, 9 mai 2017)

Il est rapidement apparu lors de l'enquête que la capacité de dénonciation de ces utilisateurs reposait sur un procédé spécifique. Il n'est pas question de faire de longues justifications, ni de longues argumentations, mais une dénonciation qui tient en 280 caractères. Inévitablement, l'élément de preuve et la mise en contexte doivent être concis. C'est donc par de multiples méthodes d'inscription que ces utilisateurs établissent un rapport direct avec la dénonciation (voir figure 7.3. pour un exemple). L'action est généralement résumée en une phrase : « Islamic State Target ». Pour signifier la cible, ils utilisent des *hashtags* comme #Daesh ou #ISIS. Ils exposent le compte suspect en le taguant par la fonction Twitter @. Par ce fait, l'utilisateur présumé jihadiste est informé qu'il est la cible d'une accusation. Par ailleurs, certains de ces internautes peuvent aussi prendre un rôle supplémentaire en rappelant la sanction future du jihadiste, c'est-à-dire son exclusion de la plateforme.

L'acte accusatoire peut faire état de diverses infractions, comme celui d'avoir enfreint les termes de service de la plateforme ou celui d'avoir piraté des comptes Twitter dormants. Quant au style, il peut être de plusieurs ordres. Certains adoptent un style épuré et simple, qui se limite à inventorier sous forme de listes des comptes jihadistes. D'autres ajoutent une capture d'écran qui sert de preuve à l'infraction commise. L'activité de dénonciation et sa mise en scène vont dans certains cas au-delà du simple signalement. Ces internautes peuvent aussi se livrer à du travail de contre-propagande humoristique en produisant du contenu parodique et moqueur (voir figure 7.4.), et parfois pornographique.

La dénonciation met ainsi en relation trois éléments invisibles les uns pour les autres : 1° le dénonciateur, 2° l'accusé, 3° le juge. Si on traduit littéralement : le dénonciateur est un compte Twitter anonyme, l'accusé est un compte Twitter jihadiste et celui à qui revient la dénonciation est un dispositif technique.

Figure 7.3. Exemple de signalement d'un compte dormant Twitter piraté par un militant de l'État islamique. L'auteur a ainsi pris le soin d'ajouter en gras la mention « hacked account » et d'entourer la date de création du compte de juin 2014. Cette publication sur Twitter date du 21 juillet 2017.

Figure 7.4. Ce mème part d'une capture d'écran d'une vidéo officielle de l'État islamique. On voit ici un jihadiste devant un ordinateur qui démontre une émotion peu enjouée. Le texte « Alhamdulillah where is my account » s'accorde à l'émotion du jihadiste face à la contestation que son compte a été supprimé. Ce mème a été diffusé sur Twitter le 4 juin 2017.

En réclamant certains garde-fous à l'utilisation du dispositif technique, ces internautes ne sont pas seulement les porte-parole d'une lutte anti-terroriste en ligne. Suivant l'analyse de Boltanski (1990), nous pouvons également dire qu'ils se font les porte-parole du dispositif technique lui-même, ce qui signifie dénoncer ses manquements en ce qui concerne la manière dont la compagnie gère la modération des contenus terroristes. Il n'est pas rare que ces collectifs mettent sur le banc des accusés les compagnies, en pointant leurs difficultés à gérer les situations d'incertitudes et à apporter des solutions cohérentes. Il n'existe pas une méthode unique pour effectuer ces dénonciations. Ces internautes utilisent des moyens divers pour rendre visibles les faiblesses du dispositif techniques.

Par exemple, certains collectifs comme CtrlSec tiennent des statistiques mensuelles concernant le nombre de suspensions effectuées par Twitter au cours du mois. Malgré que ces statistiques ne soient pas officielles et qu'il existe de nombreuses incertitudes sur la manière dont elles sont compilées, elles révèlent toutefois une volonté d'évaluer la modération de Twitter en la comparant à ses performances passées. Prenons le *tweet* de CtrlSec qui fait mention des statistiques du mois de juin 2018. Ce dernier fait le constat que l'État islamique reste présent sur Twitter et que sa propagande est en légère hausse. Plutôt que de se limiter à donner les chiffres de la modération, CtrlSec formule aussi certains constats en matière de suspension. Ils ont notamment trouvé que la modération est plus rapide pour des comptes tenus par des humains que par des *botnets*. Cette conclusion est largement confirmée par nos observations. D'ailleurs, ces comptes étaient d'abord restreints en raison d'activités inhabituelles, avant d'être suspendus. Cela pointe ainsi quelque chose de crucial : les entités humaines et non-humaines ne sont pas toujours égales devant la modération.

En revanche les « sanctions » imposées par les plateformes, ce sur quoi elles établissent la régulation de la plateforme, ont été profondément critiquées par ces utilisateurs. À ce titre, le collectif CtrlSec condamne vivement les « restrictions temporaires » que Twitter effectue en guise de non-respect des règlements. Avec clarté, CtrlSec expose l'une des principales faiblesses de ce type de solution : les contenus continuent à circuler en dépit de leur sanction. Pour asseoir son propos, c'est de nouveau sous le registre de la preuve que le collectif argumente. Sans nul doute, le collectif cherche une nouvelle fois la concision en se limitant à lister les comptes qui ont continué à diffuser le contenu d'un compte soumis à une « restriction temporaire ».

Figure 7.5. À gauche, exemple du nombre de comptes Twitter suspendus et comptabilisés par CtrlSec pour le mois de juin 2018. À droite, exemple du type de critique effectué par CtrlSec concernant les restrictions temporaires effectuées par Twitter. Ce tweet a été publié en date du 18 avril 2018.

Pour résumer, cette section démontre plus largement que la prépondérance des algorithmes pour détecter automatiquement les contenus ne tarit pas le désir de certains internautes de prendre le rôle de justicier et de porte-parole de la lutte anti-terroriste en ligne. Par ailleurs, ces utilisateurs ne se soumettent pas au plan initial du dispositif technique. Ils ne se limitent pas à signaler les contenus jihadistes, mais abordent la question de la responsabilité du dispositif technique. Ils l'évaluent, ils le critiquent. Ils se saisissent d'un ensemble de graphes, d'images, de preuves pour fixer les failles et les incompétences techniques. En d'autres termes, ils participent à jeter le discrédit sur la plateforme numérique qui doit être constaté par tous.

7.4.2. Répondre à la dénonciation, par la dénonciation

Face aux signalements quotidiens de ces « traqueurs » de jihadistes, les militants de l'État islamique ont procédé à un nouveau positionnement stratégique, pour endiguer ces menaces. Tout comme les anti-jihadistes, l'État islamique trouve en la fonction de signalement un allié de taille. Sans grande originalité, ces derniers usent des méthodes similaires que leurs adversaires. À ce titre, les militants de l'État islamique effectuent de faux signalements des comptes anti-jihadistes par le biais de comptes gérés par des humains ou des *botnets*. On assiste ici à une inversion du dispositif de signalement et de sanction. L'objet technique donne ainsi la mesure des relations en établissant des rapports de force entre différentes communautés qui se combattent à coups de signalement hostiles. Celui qui en sort vainqueur

est celui qui arrive à faire taire l'autre. Toutefois, jusqu'à présent aucune de ces deux communautés n'a été réduite à un mutisme absolu.

Pour déployer leur arsenal de signalement, le collectif utilise différentes méthodes. Lorsque l'action est conduite par des militants de l'État islamique qui se spécialisent dans ce type de combat, ces derniers emploient le même format de dénonciation que leurs adversaires. C'est une réplique directe à l'auteur de l'offense. Ils ne prennent pas l'allure de partisans de l'État islamique, mais adoptent une apparence neutre ou alors se réapproprient les codes des anti-jihadistes. Ce qui change : la cible du *tweet*. Le compte à signaler est maintenant celui de l'internaute qui reporte les abus à Twitter.

Prenons pour exemple le cas de l'utilisateur @aliiiice5. Compte dormant piraté par un partisan de l'État islamique, sa nouvelle fonction est de signaler des comptes anti-jihadistes. Malgré une photo de profil en apparence banale, il apparaît rapidement à l'observateur que ce compte se dédie à signaler des comptes anti-jihadistes. Cette activité de signalement, en apparence invisible, est matérialisée par la mise en scène de ses actions et de ses victoires.

Figure 7.6. Capture d'écran de l'historique de signalement de @aliiiice5 publiée sur Twitter le 25 février 2018.

L'utilisateur fait un usage abondant de la capture d'écran pour témoigner de ses efforts dans ce combat. Les captures d'écran sont dédiées à ses résultats et aux pertes de l'ennemi, comme l'atteste la figure 7.6. On en trouve certaines qui listent les victimes et les comptes suspendus, et d'autres où Twitter est interpellé pour rétablir le compte erronément suspendu. @aliiiice5 rend également compte de ses efforts en démontrant le nombre de comptes signalés au cours des dernières heures, ce qui donne une idée à l'observateur du temps qu'il investit. La capture ci-dessus montre que @aliiiice5 a effectué pas moins de 100 signalements au cours des dernières heures. La quantification de ses actions renforce ainsi la crédibilité de son investissement.

Les militants de l'État islamique appliquent également ces opérations à des comptes suspects pour mener des campagnes de signalements plus massives. Mener une attaque de signalements de masse ne demande pas seulement des techniques. Elles requièrent de la préparation, des stratégies et des mises en scène. Le militant de l'État islamique intervient ici comme stratège. Il faut qu'il crée de faux comptes et qu'il leur donne une apparence. Dans certains cas, c'est ici que la tromperie continue. Le partisan détourne les noms et les codes de leur adversaire. En somme, il produit une série de faux comptes à l'identique de l'ennemi. Les victimes associent régulièrement ces comptes suspects à des *botnets* et ils produisent des *tweets* et des documents pour dénoncer ces pratiques.

> Les bots #DAESH, c'est comme les poux, ça se multiplie et ça devient une plaie si pas traitée rapidement
> Des dizaines de bots détournant notre nom/logo pour harceler
> Pdt ce temps @TwitterSupport
> Seule réponse : Pas de violation de TOS (Twitter, 12 mars 2018)

De manière plus détaillée, certains collectifs publient un suivi quotidien de ces attaques, qui peuvent s'étaler sur plusieurs jours et être menées par des centaines de comptes suspects, qui se réapproprient souvent le nom du collectif.

En supprimant les comptes massivement signalés par l'État islamique, cela démontre que le dispositif technique s'avère être extrêmement mauvais pour différencier les nuances et le contexte. En d'autres termes, il n'accorde aucune importance au dénonciateur. Ce qui compte pour l'algorithme, c'est le nombre de signalements massifs effectués. Toutefois comme nous l'avons vu au chapitre 5, il est difficile d'établir si les erreurs de suspension sont le résultat d'une pure négligence, d'un algorithme défectif ou des erreurs des équipes de modération. Le dispositif technique rend totalement opaques ses failles et ses causes.

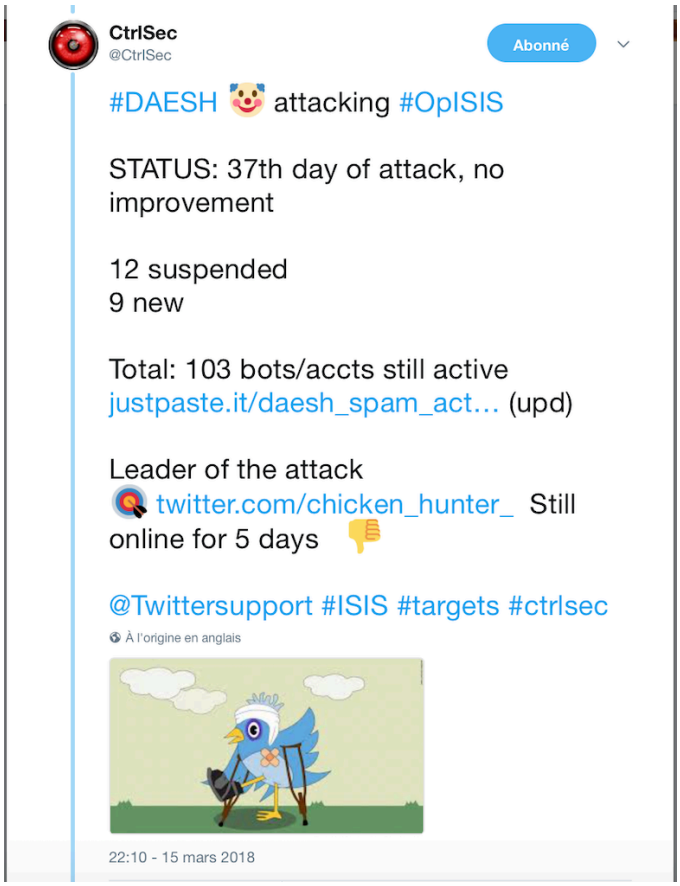

Figure 7.7. Dénonciations de la part de CtrlSec FR via CtrlSec de la création de faux comptes CtrlSec FR.

L'excès même de ces failles fait naître une controverse : celle que Twitter suspendrait ou bloquerait de nombreux activistes et qu'elle laisserait les attaques prospérer en dépit des nombreux *tweets* d'avertissements et de signalements. De là, naît un sentiment d'injustice de la part de ces collectifs et internautes qui luttent contre la propagande de l'État islamique en ligne. Ils multiplient leur appel auprès de Twitter pour exposer la situation. Ils dénoncent son extrême passivité face à ces opérations qui semblent totalement lui échapper. L'un des exemples les plus évocateurs est sans doute la lettre ouverte à Damien Viel, Directeur Général de Twitter France, produite par les Katiba des Narvalos :

COMMUNIQUÉ DE PRESSE
10 mars 2018
Lettre ouverte à Damien Viel, Directeur Général de Twitter France.

Monsieur Damien Viel,

Depuis 2015, nous luttons contre la propagande jihadiste sur les réseaux sociaux. Bien que Twitter se soit considérablement assaini depuis trois ans, grâce, notamment, au travail des activistes anti-EI, aux pressions des pouvoirs publics, et, finalement, à la prise de conscience de Twitter, nous assistons depuis un mois à une inquiétante recrudescence d'activité de comptes se

> réclamant de la mouvance jihadiste. Nos comptes, ainsi que 300 autres liés à l'opération OpISIS (détails dans le document en lien ci-dessous), sont pris pour cible et suspendus les uns après les autres. Des attaques ciblées, annoncées au préalable, puis revendiquées publiquement.
>
> Nous déplorons la passivité du support Twitter. Hier, 9 mars, c'est Abou Portant (@Abu_Portant, parodique, 3400 abonnés) qui s'est vu suspendu, ciblé par un compte pro-EI, signalé à maintes reprises depuis une semaine au support Twitter, mais toujours en ligne. Le 4 mars, c'était Harissa (@abuharrisa), toujours suspendu à ce jour, malgré les protestations et centaines de retweets et messages de soutien. Abou Zilleur (@AbouZilleur_) a été pris pour cible le 8 mars par un compte signalé au Support par @CtrlSec/@CtrlSec_FR et des dizaines d'activistes, mais toujours actif. Etc.
>
> Nous vous prions d'intervenir pour que les comptes soient rétablis, et, conformément aux conditions d'utilisation de Twitter, que ceux les ciblant soient enfin suspendus. Auquel cas, nous disparaîtrons, et l'histoire retiendra qu'en 2018, des sympathisants du jihad ont eu raison d'une initiative citoyenne contre la propagande terroriste, cela dans l'indifférence de Twitter.
>
> Veuillez recevoir, Monsieur Damien Viel, l'assurance de nos sentiments les meilleurs.
>
> Katiba des Narvalos

Les avertissements des Katiba des Narvalos et de CtrlSec font toujours état des mêmes plaintes : des centaines d'utilisateurs anti-jihadistes sont harcelés, attaqués, bloqués, suspendus par des comptes détenus par des pro-jihadistes qui continuent de prospérer.

> Les comptes de harcèlement et signalements abusifs des pro-jihad pullulent en toute impunité. Ils continuent de harceler leurs cibles, d'annoncer préalablement leurs opérations, puis de langer leurs signalements massifs et enfin revendiquer leurs trophées obtenus grâce à Twitter.[115]

En tant que porte-parole du dispositif technique, ces collectifs condamnent vivement la manière dont il est géré. Ils accusent notamment Twitter « de ne pas travailler sérieusement », de faire des « erreurs grossières récurrentes », d'avoir une « forme de complicité indirecte avec les jihadistes » et d'avoir des équipes de modérations incompétentes. De plus, les collectifs critiquent de manière virulente le manque de volonté de Twitter à mettre en place de nouvelles solutions.

> Plusieurs solutions potentielles simples existent depuis longtemps. Les équipes Twitter ont toujours refusé de les prendre en compte en restant enfermées dans leur tout d'ivoire, préférant miser sur la sous-traitance low-cost de la modération par des équipes non formées et des algorithmes dont on constate

[115] *Mémorandum attaques Twitter*, Katiba des Narvalos, 10 mars 2018.

encore les failles.[116]

En pointant la responsabilité de Twitter dans la recrudescence des comptes jihadistes, CtrlSec pousse ses avertissements plus loin. Si le dispositif technique continue à rester passif face aux agissements de l'État islamique, il devra en subir les conséquences. Le collectif n'envisage pas des sanctions pénales, mais des sanctions économiques : que les actionnaires se désistent face à environnement toxique et dysfonctionnel.

> Its' looks like TWITTER just don't care about the SAFETY of their users. We hope that the Twitter's shareholders will be made fully aware of the type of dysfunctional business they support[117].

7.4.3. De la dénonciation à l'altercation

Nous avons observé lors de notre enquête que les opérations de dénonciation peuvent basculer en altercation entre pro et anti-État islamique. Nous avons analysé 46 conversations Twitter (ou bribes de conversations) entre des pro État islamique et des anti-jihadistes impliqués dans l'#OpISIS. Elles ont été analysées selon plusieurs dimensions : les acteurs de l'interaction, les contenus, les dispositifs d'inscription et la dynamique de la conversation. Certaines conversations étaient très courtes, ne contenant pas plus de deux *tweets*, alors que d'autres en contenaient jusqu'à une vingtaine.

Nous commencerons par considérer un court extrait d'une conversation afin d'illustrer certains des procédés par lesquels les deux communautés interagissent et se confrontent. Ici, la discussion a lieu entre un partisan de l'État islamique (@ihsgshs2k) qui est régulièrement la cible de signalements et un Anonymous (@anon-985ti) connu de l'#OpISIS. La discussion commence à la suite d'un signalement de @ihsgshs2k pour contenu terroriste. Le militant pro État islamique interpelle l'internaute qui l'a signalé pour montrer qu'il est de retour. Un acte de provocation auquel certains militants de l'État islamique aiment régulièrement se livrer.

> Twitter, 22 mars 2017, discussion numéro 13 :
>
> <@ihsgshs2k > @anon-985ti @TwitterSafety @Support @Twitter 😂😂😂😂😂😜
>
> <@anon-985ti> @ihsgshs2k @TwitterSafety @Support @Twitter are you laughing for the same reseon I m laughing mrs unbeliever ☺

[116] *Mémorandum attaques Twitter*, Katiba des Narvalos, 10 mars 2018
[117] Rapport CtrlSec « *About @TwitterSupport consistency and standards when dealing with abuses of ISIS terrorist accounts* », 21 février 2018

<@ihsgshs2k> @ anon-985ti @TwitterSafety @Support @Twitter And why you leugh mr.unbeliever ? ☺

<@anon-985ti> @ ihsgshs2k @TwitterSafety @Support @Twitter because soon I will be talking to you on another account. 😂😂😂😂 you will be suspended again 😂😂😂

Ce bref passage témoigne de quelque chose que nous avons souvent observé lors des interactions entre ces deux communautés, une sorte de fausse proximité qui se traduit par de la moquerie, de l'humour et de la provocation. Il faut également dire qu'il s'agit souvent des mêmes utilisateurs anti et pro État islamique qui se confrontent. Nous étions en quelque sorte face à un cercle d'initiés de « signaleur-signalé ».

Twitter, 5 avril 2017. Discussion numéro 28 entre @yuhzzqw et @Anon3tww. @yuhzzqw connue sur la toile, cette militante de l'État islamique, souvent traquée et suspendue, interagit régulièrement avec les Anonymous. La discussion a commencé à la suite d'une publication qui appelle à signaler le nouveau compte de @yuhzzqw.

<@Anon3tww> 5x up today for real [parlant du nombre de fois où l'utilisatrice est réapparue]

<@yuhzzqw> Pas 5 mais 15 😎 [Traduit de l'arabe]

Plus tard, lors de l'interaction @yuhzzqw rappellera à son interlocuteur qu'elle sera de retour.

<@Anon3tww> No worries soon twitter will suspend your ass again and you wont have to see her… [Parlant d'un autre partisan de l'État islamique faisant souvent l'objet de signalement]

<@yuhzzqw>, Mais je serai de retour 🤗😎[Traduit de l'arabe]

Dans la plupart des interactions analysées, l'échange entre ces communautés se solde par la transgression et le spectacle. Pour les membres se revendiquant d'Anonymous et autres internautes anti-jihadistes, ils utilisent la pratique du *trollage* où le *Lulz* était la force motrice de leur action. Le *Lulz* est défini par Coleman (2016) comme un « état d'esprit propre à l'humour noir des Anons ; dérivé de *lol*[118] ». Les partisans de l'État islamique réceptifs aux provocations de ces internautes répondent par des menaces et des images d'une extrême violence. Comment ces échanges d'hostilité se matérialisent-ils ? Principalement à travers des querelles d'images. Une pratique que nous avons déjà vue à l'œuvre sous forme automatisée dans le chapitre 5. Une nouvelle fois, l'échange d'hostilité se réalise par des dispositifs d'« inscriptions numériques ». L'avantage pour les deux camps est que ces dispositifs

[118] *Laugh out loud*, pouvant se traduire par « mort de rire », mdr.

d'inscription ne les feront jamais manquer de matériel. GIF, mème, émoticônes, captures d'écran, images, séquence de vidéos, tous ces matériaux leur permettent d'effectuer des mises en scène peu élaborées, aux codes plus décontractés et plus simplistes. Si le texte est une dimension importante des échanges, il est complété par des dispositifs visuels. Parfois, seule l'image parlera. Prenons le cas de cette conversation qui découle de nos notes de terrain :

> Z. est de retour. Comme d'habitude, son arrivée ne passe pas inaperçue au sein des anti-jihadistes. À peine arrivés, ces derniers sont prêts à effectuer leur énième signalement de la journée en ce qui la concerne et à attaquer avec leur stock d'images. Z. le sait, son compte sera prochainement suspendu. Elle n'abandonne pas et publie une série de *tweets*. Une publication, celle d'un passage d'une vidéo officielle de l'État islamique, suffit à attirer l'attention des « traqueurs » jihadistes. C'est M. qui ouvre les festivités, en publiant une simple photo en noir et blanc d'un doigt d'honneur. A. suit. L'hostilité continue cette fois-ci avec une photo où l'on voit très clairement le drapeau de l'État islamique en train de brûler. A. ne s'arrête pas là, c'est sous le registre de la caricature qu'il poursuit. Une caricature qui s'attaque au mythe des 72 vierges offertes aux martyres et une autre qui utilise la métaphore d'un sac à ordure pour représenter les combattants de l'État islamique. À chacune de ses provocations, Z. prendra le soin de répondre. Sans trop d'originalité, sa réponse est sans équivoque et utilise à chaque fois la même image de décapitation. L'image est celle d'une séquence d'une vidéo de propagande officielle de l'État islamique. C'est ainsi par une simple capture d'écran que la séquence incarne une nouvelle forme d'inscription. Le choix du moment de la capture d'écran n'est pas anodin et est particulièrement bien choisi pour effectuer un effet de sidération auprès du spectateur. Sur la capture d'écran, on peut voir deux ennemis de l'État islamique vêtus d'une combinaison orange allongés au sol. Leur gorge est béante. Les jihadistes vêtus d'une tenue noire se maintiennent assis sur leur victime et terminent l'action de décapitation. L'image capture ainsi le moment de torture et de supplice. L'excès de violence dûment constaté au sein de cette image, est une pièce de la puissance du collectif. [Notes de terrain d'une conversation Twitter entre pro et anti-jihadiste, 11 mars 2017]

Ce passage illustre la manière dont les querelles se déroulent entre les partisans de l'État islamique et les anti-jihadistes. Les deux communautés utilisent des stratégies et des tactiques pour se déstabiliser l'une et l'autre. Dans une aisance et une désinvolture, les anti-jihadistes s'amusent à mettre les jihadistes dans des situations particulièrement humiliantes et dégradantes. Par une série de mèmes, ils s'attaquent aux emblèmes sacrés de l'État islamique, jouent avec les interdits religieux de l'islam et ridiculisent leur chef mort Abu Bakr Al-

Baghdadi. Parfois, ils rappellent la loi et les sanctions en ce qui concerne l'apologie du terrorisme sur internet. On pouvait alors voir une image sur laquelle apparaissait l'intérieur d'une prise, des portes et des barreaux, avec le message suivant :

> MÊME SUR LES RÉSEAUX SOCIAUX, ON NE PLAISANTE PAS AVEC LA LOI. FAIRE L'APOLOGIE DU TERRORISME EST PUNI DE 7 ANS DE PRISON ET DE 100 000 EUROS D'AMENDE. (Pour en savoir plus, cf. article 421-2-5 du code pénal). #STOPDJHADISM

Quant aux militants de l'État islamique, ils préféreront riposter par des images brutes. Il n'est pas question d'esthétisme, de créations, de détournements de contenus, juste des images en ce qu'elles ont de plus réel, abjectes et terrifiantes. Ces « images intolérables », pour reprendre l'expression de Rancière (2008), livrent à son adversaire une véritable performance de la violence. La particularité des images sélectionnées par l'État islamique est qu'elles nous montrent le supplice tel quel. Elles capturent la violence en train de se faire. Ce sont ces excès de supplices qui rythmeront les échanges en ligne avec leurs adversaires. Pour amplifier l'effet, certains jouent avec les dimensions de l'image, en faisant un usage abondant de l'option « gros plan ». Bien entendu, tout comme les anti-jihadistes, l'État islamique a un stock d'images non négligeables et sait varier ses ripostes. À cet arsenal d'épouvante, les militants de l'État islamique peuvent aussi très bien rappeler le traumatisme des attentats subis en occident.

Eu égard à ce qui précède, nous pouvons voir plus nettement comment le rapport entre ces deux communautés se traduit par de courtes ou de longues chaînes visuelles. Il s'agit d'une surenchère d'images grotesques et humiliantes pour les uns et d'images dans ce qu'elles ont de plus violent, abject et extrême pour les autres. Point de finesse pour les deux communautés. Plus c'est grossier et brutal, mieux c'est. Tout l'intérêt est de publier du contenu qui offusque l'adversaire. Il faut attirer le regard. Ces luttes iconographiques subissent ainsi des sélections, des extractions, des amplifications, des réductions et nécessitent un ensemble de véhicules matériels.

Figure 7.8. Image moquant les interdits religieux de l'Islam. Ici une photo de bacon en cœur.

Figure 7.9. Mème moquant l'État islamique en mettant en scène leur stupidité en lettre majuscule appuyée par deux images où on voit un jihadiste tomber en tirant et un nain-combattant posant devant le drapeau de l'État islamique.

Figure 7.10. Images mettant en vis-à-vis un phacochère et un combattant de l'État islamique posant fièrement devant son drapeau.

Figure 7.11. Mèmes mettant en scène l'état islamique et ses symboles dans différentes scènes humiliantes et dégradantes.

Tableau 7.1. Sélections de mèmes moqueurs et insultants à l'égard de l'État islamique publiés en 2017 sur Twitter.

Dans cette bataille, l'image n'est toutefois pas le seul vecteur pour signifier la terreur à ses adversaires. À celle-ci, s'ajoute parfois une succession d'émoticônes, qui représentent par exemple les tactiques d'attentats privilégiées par l'État islamique : le camion, le couteau, l'arme à feu, la bombe.

Figure 7.12. Suite d'émoticônes produite par une militante de l'État islamique dans le cadre d'une interaction avec des « traqueurs » de jihadistes.

Ces courtes figurations symboliques, accessibles sur à peu près tous les systèmes d'exploitation et plateformes numériques, ont fait l'objet d'une appropriation imaginative de

la part des partisans de l'État islamique. De façon sans doute plus élaborée que chez les anti-jihadistes, dont l'émoticône de prédilection exprimant leur registre d'humour est l'émoji « rire aux larmes » (😂), les partisans de l'État islamique ont substitué des suites d'émojis aux mots pour exprimer leur menace ou leur mépris à l'égard de leurs adversaires. Les émojis annexés au royaume de la menace jihadiste avaient maintenant un nouveau rôle, celui de signifier la terreur. Tout était bon à prendre pour compléter la panoplie du « prêt-à-menacer ». De l'émoji « camion » qui renvoie pour ses concepteurs à l'univers du transport, il passe à celui de tactiques pour commettre des attentats. Les émojis tels que la bombe et l'arme à feu sont quant à eux plus faciles à intégrer dans le répertoire violent et menaçant.

Figure 7.13. Exemple de lignes d'émoji constituées par un partisan de l'État islamique, en réponse au signalement d'un Anon. Nous avons 7 types d'émojis : doigt d'honneur, bombe, deux sortes de couteaux, arme à feu, cercueil et lion[119]. En 41 émojis, l'auteur du *tweet* assure un style hostile et menaçant à l'encontre de l'Anon.

Figure 7.14. Exemple d'émoji signalant le mépris d'un partisan de l'État islamique en réponse au signalement d'un « traqueur » de jihadistes, avec la mention « specially for you ».

Mobiliser un registre de menaces passe ainsi par la délégation de la parole à un ensemble d'éléments graphiques. L'expression se mue dans le dispositif technique qui permet de créer un système représentationnel. L'émoticône *est* un représentant de l'expression et *a* des représentants pour les faire exister de différentes manières.

Malgré l'agressivité, les insultes et les menaces que s'échangent ces deux communautés, elles savent aussi se montrer amusantes, en s'adonnant au registre de l'humour. Nous avons par exemple intercepté un échange entre une militante de l'État islamique et un Anon, qui témoignaient d'une extrême légèreté. La militante de l'État islamique commence par répondre au *tweet* qui la signale par un simple « hi 😊😂 ». Pour signifier le départ imminent de la militante de l'État islamique, l'Anon publie un GIF où l'on voit deux femmes blanches aux cheveux blonds, vêtus d'un débardeur faisant apparaître leur ventre et leur décolleté et fait au

[119] Le lion est un symbole important dans la culture jihadiste. Reproduit sur de nombreux visuels, il signifie l'honneur, la force, le courage. De manière plus générale, le lion a été associé aux premiers compagnons du prophète et à leur action héroïque sur le champ de bataille (Brachman et Boudali, 2006).

revoir de la main. La militante de l'État islamique mobilise également le registre du GIF, cette fois-ci en ne puisant pas dans le répertoire jihadiste, mais dans celui de la référence *mainstream*. Le GIF choisit par celle-ci affiche un Pikatchu faisant signe de la main et où l'on peut lire de la tristesse sur son visage. On comprend très vite que les deux internautes ont tous les deux puisé dans la même banque de GIF Twitter à partir du mot-clé « BYE ».

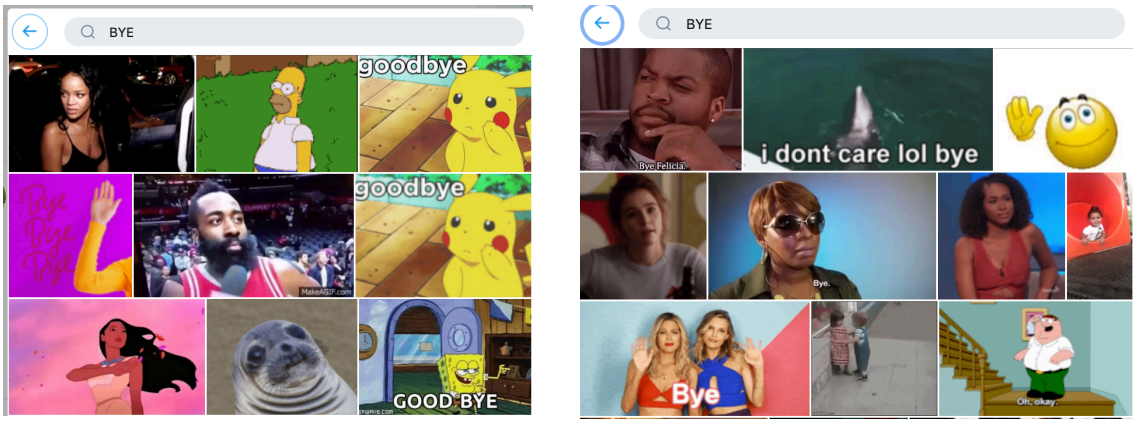

Figure 7.15. Exemple de GIF proposé par Twitter, pour la catégorie BYE. Capture d'écran datant du 30 avril 2019.

Au cours de la conversation, la militante de l'État islamique signale à son interlocuteur être « verry happy today 😃😃 ». Plusieurs anons se saisissent de ce moment pour lui rappeler qu'elle sera bientôt suspendue. Cela ne perturbe pas pour autant la militante de l'État islamique qui leur signifie que leur effort est vain étant donné qu'elle sera de retour. Elle communique ainsi sur une dimension de réalité ; celle de sa persévérance dans la lutte contre l'invisibilité.

> @wolf-934 : right away you won't be so happy, your account will go down
>
> @ anon-985ti : I hope you are very happy while setting up your new account.. enjoy this one while it last ☺
>
> @ciips8189 : 😁 but I'm back
>
> (Conversation Twitter, 20 avril 2017)

Ce type d'échange dénote avec ceux précédemment évoqués. Plutôt que d'exprimer des menaces, l'internaute préfère ironiser cette fois-ci sur son sort. L'humour en vient à circuler symétriquement entre les différentes communautés. Les conversations constituent ainsi une source de données extrêmement riche. Premièrement, elle nous montre la diversité des

échanges qui s'établissent entre des communautés hostiles l'une envers l'autre. Ensuite, si les registres mobilisés s'enracinent dans la culture de chacune des communautés, certains traits communs peuvent toutefois les relier : l'humour et le goût pour la provocation. Troisièmement, nous avons vu que les dispositifs d'inscription sont multiples et permettent à chacune des deux communautés de mener son combat et défier son rival. Le différend se solde ainsi par une escalade continue de contenus qui s'inscrivent principalement dans une lutte iconographique.

Conclusion : Visibilité et restriction

Ce chapitre s'est proposé d'explorer les contraintes et les différentes forces ennemies qui contrecarrent le projet de visibilité de l'État islamique. Par ailleurs, la relation n'étant pas unilatérale, ce chapitre s'est aussi intéressé à la manière dont l'usager jihadiste a « mis à l'épreuve » le dispositif technique. L'usage des plateformes par les jihadistes a remis en avant-plan les questions relatives à la régulation du réseau. Face à la menace terroriste, les gouvernements ont eu un motif suffisant pour intervenir dans le contrôle de l'information. Ces derniers ont contraint les plateformes à chercher des solutions nouvelles et plus satisfaisantes que celles qu'ils possédaient. La solution de l'automatisation a été mise sur le devant de la scène.

En matière de modération des contenus, il s'agit d'un nouveau franchissement pour les plateformes. Les pratiques de détection automatisée de contenus sont récentes dans leur histoire et n'en sont encore qu'à leur balbutiement. Toutefois, il ne semble pas qu'il faille y voir un progrès, à proprement parler, mais plutôt de changements et de renforcements de potentialités internes aux dispositifs techniques (Simondon, 1958). C'est en partant de ces potentialités qu'un être technique nouveau est apparu en tant qu'actant. Le dispositif technique s'est réinventé et restructuré dans sa modération, sous couvert d'un discours solutionniste. Pour ainsi dire, la modération crée un nouveau programme d'action pour la plateforme et un anti-programme pour le jihadiste, à savoir l'empêcher de se fixer à l'objet technique. Ainsi, le jihadiste qui bénéficiait d'une posture d'utilisateur est maintenant mis en cause par le dispositif technique qui insère son usage dans une chaîne de filtrage qui se veut plus efficace et plus proactive. Le dispositif change de fonction, à la base conçue comme espace d'expression, il favorise un environnement hostile à des idées particulières.

Si, dans le chapitre précèdent, nous avons vu en quoi les algorithmes favorisent la visibilité,

celui-ci montre que l'algorithme peut aussi réduire l'utilisateur à l'invisibilité. Ainsi, les algorithmes sont à la fois source de puissance et menace. Ce qu'il y a de particulier ici, est la monopolisation par les grandes plateformes numériques de la sophistication de la modération. Dans ce contexte, elle est prise dans des nouvelles relations de pouvoir d'une grande complexité. Ces pouvoirs s'affilient à des stratégies et des agencements qui sont à la fois coûteux et opaques. Ils nécessitent une vue totalisante et globale des internautes et de leurs interactions. Ils les historicisent, leur assignent des catégories. Ce faisant, nous pouvons voir qu'un important système d'alerte existe entre le militant jihadiste et le dispositif technique. La relation devient celle d'un signal permanent, où chaque transfert d'information par l'usager jihadiste permet à la machine d'effectuer un repérage de signaux pour effectuer sa catégorisation. Une fois la catégorisation validée, le jihadiste est alerté de son statut et de sa sanction. Si, du côté de la technique, il s'agit de réduire le champ des indéterminations, du côté du militant jihadiste, il s'agit d'être plongé dans une incertitude technique.

Dans un dernier temps, ce chapitre s'est intéressé à la manière dont le signalement informatique fonctionne concrètement dans le monde du militantisme, c'est-à-dire en quoi il a été détourné de son rôle initial pour devenir un objet de lutte entre différentes communautés. L'outil de signalement subit en quelque sorte une nouvelle traduction : il passe d'une mission de protection de la communauté à une mission visant à faire taire l'ennemi. La première formulation en appelle à la morale et à la responsabilité des internautes. Elle est nécessaire pour que la plateforme numérique reste un lieu agréable et convivial pour tout le monde. Un objectif dont s'est emparé le collectif Anonymous et d'autres utilisateurs pour lutter contre la propagande jihadiste en ligne. L'usage de cette fonctionnalité ne pacifie pas pour autant l'espace : elle renvoie à des disputes, des conflits et des vengeances. En somme, ce n'est plus la fonctionnalité pacifiée imaginée par ses concepteurs, mais celle d'un champ de bataille.

Cela nous amène à la deuxième formulation qui en appelle à l'offensive et à la défense. Mentionnons que le dispositif de signalement est indifférent à la fonction qu'on lui assigne : n'importe qui peut signaler un compte, pour des motifs qui lui sont propres. En cela, la fonction et les propriétés de base de l'outil peuvent facilement lui échapper, laissant le champ au déploiement d'usages pervertis. Nous avons en effet vu que l'outil de signalement favorise le déploiement de stratégies pour organiser des signalements de masse. L'art de mener des signalements de masse consiste en ceci : signaler le plus de fois possible un *tweet* ou un profil pour son caractère offensant afin que l'algorithme le repère.

Conduire ce type d'actions nécessite de construire un appareillage technique qui rend compte de comportements délétères. Celui qui mène l'offensive doit effectivement détenir une multitude de faux comptes. Ce qui a le plus d'importance dans ces attaques, c'est de contraindre l'ennemi à l'invisibilité pendant un certain temps. Signaler un compte ne signifie pas pour autant que l'invisibilité perdurera dans le temps. En cas d'erreur, le compte peut être restauré ou alors l'utilisateur peut se créer un nouveau compte. Toutefois, ces exclusions temporaires ou définitives provoquent la rupture et la dislocation eu égard au dispositif technique. Il s'agit de briser des alliances et d'exclure l'adversaire du jeu de riposte. L'ennemi doit plutôt se battre pour réapparaître en ligne tout en sachant que le risque de suspension continue de planer.

Chapitre 8 : Résister à la modération

Dans *Le mythe de Sisyphe*, Camus écrivait qu'« il vient un temps où il faut choisir entre la contemplation et l'action » (1942 : 119). Confronté à la modération, plutôt que de capituler, le collectif a choisi l'action. L'action de lutte. C'est sur ce point que porte le dernier volet de nos résultats. Il s'agit de se demander comment le collectif tente de résister au pouvoir disciplinaire des technologies du web. Dans ce chapitre, il sera donc question de nouveaux modes d'engagement avec le dispositif technique. Des modes d'engagement qui, précisons-le d'emblée, diffèrent radicalement des usages communs. Il est un fait : l'activité de modération a contraint les militants à élaborer quotidiennement des tactiques qui assurent au collectif de rester visible en ligne. Ce chapitre se penche ainsi sur la manière dont le collectif contraint le dispositif technique à reprendre son rôle d'hébergeur de contenu.

L'objectif de ce chapitre sera de montrer les limites de cette prétention à « discipliner l'utilisation » (Thévenot, 1993) de la part des firmes propriétaires. Nous passerons en revues plusieurs tactiques que le collectif a mises en place pour contourner la censure. Nous verrons toutefois que cette riposte a aussi ses limites. C'est pourquoi il est préférable de parler d'un affrontement et d'une lutte dynamique entre les plateformes numériques et les usagers.

Nous verrons dans un premier temps comment le collectif scénarise son retour sur la plateforme et cherche à défier le dispositif technique. Nous analyserons ensuite les différentes tactiques mises en place par le collectif pour réduire les effets néfastes de la modération et assurer la pérennité de leur visibilité. Enfin, nous nous appuierons sur deux études de cas qui mettent de l'avant deux configurations d'usager dans un contexte où la modération est continue.

8.1. Défier le dispositif technique : *We're back again*

L'archétype du réseau technico-jihadiste est devenu celui de l'interruption et de l'incertitude. Le déplacement de posture du dispositif technique contraint l'utilisateur jihadiste à modifier le spectre de ses usages et de ses actions routinières. Il le condamne finalement à renouveler quotidiennement la même action : celle de recréer un nouveau compte.

> <@189_zarq> welcome back sisters, what happened I just your account, is this a new wave
>
> <@IRAQI7891> as usual they had suspended my account
>
> <@189_zarq> This isn't a problem for you, your great efforts is paying off as usual, don't worry I'm next
>
> (Conversation Twitter, 15 mars 2017)

Conscient de leur destin, ce n'est point la passivité et le désinvestissement qui parcourent le collectif. En réalité, le collectif a rapidement tiré profit des suspensions et en a fait une marque de fierté et de victoire.

> You are the knights in your battle in the media, and the « technology of the West » under your feet. Deleting your accounts as an enemy is for you a success and a victory[120].

En réapparaissant sans cesse sur les plateformes, le collectif s'efforce de montrer qu'il garde une position avantageuse sur les technologies du web. Si elles lui imposent des contraintes et des interdits, il démontre qu'il n'est pas voué à la discipline. Il développe l'aptitude de toujours occuper le lieu de son exclusion. C'est finalement cela l'héroïsme 2.0 : contourner les sanctions du dispositif technique et donner l'illusion de le dominer. À partir du moment où il est en mesure de réapparaître, il enseigne une chose à l'adversaire : ils sont pris d'une énergie toujours inépuisable ; ils sont là pour vaincre. En somme, ils seront toujours là malgré les suspensions.

> Message pour les mécréants qui pensent nous combattre et nous censurer… Regardez l'évidence de notre présence dans nos villes et comprenez bien la détermination des lions de France par la grâce d'Allah. Nous sommes encore là malgré vos tentatives de nous faire taire sur les réseaux. Nous trouverons toujours des moyens pour communiquer et échanger entre nous. (…) (Groupe Telegram, 21 avril 2017)

[120] Extrait d'un communiqué pro État islamique, enregistré sur Telegram le 19 juin 2017.

Le collectif assure avec entêtement qu'il est en situation de puissance et de contrôle. Il évoque tacitement le travail inutile et vain de la modération.

> I see nothing has changed, we've been doing this for years, kuffar spend billion of dollars to shut down our voices in the cyber world, and all it takes to come back is a maximum of 5 minutes, good luck. https://t.me/---- (Chaîne Telegram, 26 juin 2017)

Mais, si le collectif met à mal le pouvoir disciplinaire des technologies du web, il crée toutefois des simulacres de sa puissance. Certes, la modération n'annihile pas la présence du collectif en ligne. Cela n'empêche qu'elle a le pouvoir de le désorganiser. Chose que le collectif évince totalement de son narratif. Il préfère constituer des schémas d'actions qui articulent la mise en scène de leur retour et de leur vigueur.

Leur retour ne doit pas passer inaperçu : il faut qu'il soit nommé et mis en preuve. Il est un dire sur leur condition d'exclu. Tout comme il nomme la robustesse des troupes. En quelque sorte, le récit de leur retour définit un exclu qui revient on ne peut plus puissant. Cela commence par des mots simples tels que « we're back again » ou dans sa forme individuelle « i'm back again ». Un préalable qui allait devenir une sorte de mantra au sein du collectif. Pour rendre visible et objectivable leur suspension, certains disséminent la preuve de leur exclusion.

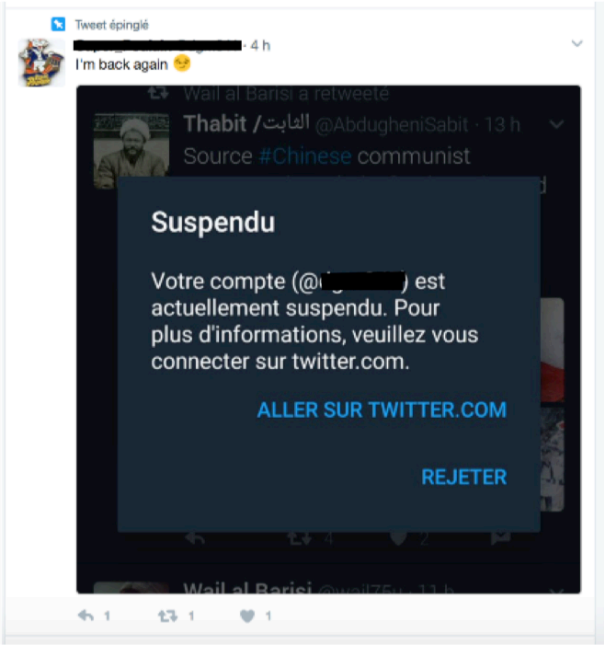

Figure 8.1. Message Twitter signalant que le compte Twitter de l'utilisateur a été suspendu. L'utilisateur a fait une capture d'écran de ce message et l'a publié sur son nouveau compte ensuite. Ce *tweet* a été publié le 25 avril 2017.

Une technique simple est de faire une capture d'écran du message Twitter qui les avise que leur compte a été suspendu, comme en témoigne la figure ci-dessus. Pour pousser la provocation plus loin, l'éliminé se targue de son retour en comptabilisant le nombre de fois dont il a fait l'objet d'une suspension. Ce chiffre peut être précis « de retour encore et toujours bi'idni Allah. Pour la 69ème fois. Honte à vous Twitter. » ou de l'ordre de l'incalculable « back after countless suspensions ». Une manœuvre qui peut d'ailleurs se prolonger dans les noms d'utilisateurs et les liens Telegram. Notons que, sans surprise, les partisans ont tôt fait de détourner le fardeau des suspensions en humour et moquerie. Le processus humoristique peut se réaliser de deux manières : par un seul utilisateur ou dans un processus collectif qui met à profit les mèmes. Dans le premier cas, quand un utilisateur publie :

> Dear spy,
> It is OK that you report the channels. But please better your timing. Don't interrupt when I am in the middle of a post. Sure, be early but not when I have already begun. (Chaîne Telegram, 4 août 2019).

C'est lui-même qui moque le dispositif de signalement. Dans le second cas, nous étions en présence d'artefacts comme les mèmes visuels. Il faut souligner la profusion des *lolcats* dans ce dispositif humoristique, qui rappelons-le ont vu le jour sur 4chan (Coleman, 2016). Les *lolcats* sont tout du moins sortis des limites du forum pour se généraliser à l'espace numérique, au point d'atteindre des révolutions de tout type. Ainsi, comme Mina le note « cat seem to have a knack for wandering into our technological revolutions » (2019 :15). Que le collectif utilise les *lolcats* ou d'autres visuels, l'intention reste la même : moquer et mépriser les actions des censeurs.

Tableau 8.1. Sélection de mèmes téléchargés sur des chaînes et groupes Telegram entre 2017 et 2018 pro État islamique qui moquent les suspensions.

Ainsi, le langage est un puissant vecteur pour signifier à son adversaire que leurs tactiques d'exclusion sont vaines et inefficaces. Par ces narrations, cela montre que le collectif n'avait pas pour seule intention de se limiter à des stratégies techniques pour réapparaître en ligne. Il fallait mettre leur destin en mot, en spectacle. En démontrant par l'ensemble de ces condensations verbales et visuelles qu'il lui est possible d'être là où on ne l'attend plus, le collectif annonce qu'il détient un système de ruses et de tactiques qui lui fournit les conditions d'une réappropriation de l'espace. Nous voici maintenant en mesure de dire que les technologies du web engendrent des luttes pour la visibilité. Se façonnent alors des unités nouvelles et inattendues, qui engagent une riposte du tac au tac contre le pouvoir disciplinaire. En un mot : le collectif pose les jalons d'un nouveau programme d'action, celui de la contre-attaque. Ils forment un écart de pratiques (De Certeau, 1990), que nous verrons plus précisément dans la section suivante.

8.2. Court-circuiter les suspensions

Pour assurer son retour, le collectif se livre à un ensemble d'opérations habiles. Sa résurgence met en branle des « tactiques de résistances » au sens qu'en donne De Certeau (1990). L'auteur indique que « la tactique dépend du temps, vigilante à y "saisir au vol" des possibilités de profit » (p. xlvi). La tactique s'inscrit dans un rapport à l'autre. Elle s'exécute par un ensemble de tours de passe-passe dans un ordre donné. Ainsi, la tactique n'a « pas la possibilité de se donner un projet global ni de totaliser l'adversaire dans un espace distinct, visible et objectivable » (De Certeau, 1990 : 61). C'est dans ce lieu contrôlé par les plateformes numériques, que le collectif doit introduire des surprises et des ruses. C'est à partir de là que nous pouvons considérer que le collectif est un candidat au bricolage. En se réactualisant dans un nouveau programme d'action, le collectif organise et bricole des solutions qui lui permettent de continuer à fonctionner et de faire circuler les flux informationnels. Le bricolage, comme forme de tactique, doit s'arranger avec le terrain que lui imposent les technologies du web. Il bricole en quelque sorte pleinement dans le champ de vision de celui qui le contrôle (De Certeau, 1990). Pour asseoir ce propos, reprenons la formule succincte de Lévi-Strauss : le bricoleur doit « s'arranger avec les moyens du bord » (1962 : 31). Les tactiques de résistance de l'État islamique sont multiples et difficiles à délimiter. Comme nous le verrons dans ce qui suit, ce sont des schémas d'opérations qui mêlent transgression, solidarité, manipulations techniques ou encore mobilité.

8.2.1. Transgresser l'algorithme

Nous l'avons vu, l'usage généralisé des algorithmes de détection automatique qui signalent plus de contenus terroristes et plus rapidement est un drame pour le collectif. Nous avons montré que l'algorithme de détection, en tant que technologie de surveillance, apporte un savoir sur les contenus et les profils délétères. En ce sens, l'activité algorithmique aménage des savoirs qui permettent de voir et de reconnaître sans arrêt le flux problématique et de le trier aussitôt. Les algorithmes donnent l'illusion d'une pleine lumière sur les flux. Illusion, car ce pouvoir de détection n'est pas infaillible. En fait, ils réagissent très mal à l'altération. Ils ne fonctionnent qu'à partir du connu. Ce que plusieurs chercheurs en intelligence artificielle ont remarqué c'est que « a range of recent studies has demonstrated that many modern machine-learning models are not robust to adversarial examples: examples that are intentionally designed to be misclassified by the models » (Dubey et al., 2019 :1). De là, la faille majeure des algorithmes : ils sont discontinus dans son efficacité. Pour cela, il ne représente pas un savoir absolu, mais bien un savoir partiel selon un enchaînement calculatoire particulier.

Celui qui connaît les failles de ce pouvoir opaque pourra le déjouer de sa trajectoire en utilisant des méthodes extrêmement simples. Certains militants ont montré qu'ils étaient conscients de la culture algorithmique qui les entoure. Ils ont dès lors mis en place des tactiques pour transgresser les algorithmes de détection. Celles-ci consistent à altérer minimalement la forme de certains contenus et images pour duper l'algorithme. En usant de cette technique, le contenu peut passer sous le radar de l'algorithme et continuer à circuler. Dans le cas de l'État islamique, une chose claire : tant qu'il continue à diffuser des images, textes ou audio non-altérés sur les plateformes, l'algorithme est gagnant. Si le collectif décide de dégrader le contenu, il sera cette fois-ci gagnant sur l'algorithme. Étonnamment, le recours à l'altération, pourtant simple à faire, n'est pas une pratique généralisée. Elle est une tactique mal connue des partisans, voire mal utilisée. Nous avons été témoins d'utilisateurs qui publiaient à la fois un communiqué altéré et sa version non altérée. Ce faisant, le profil était à nouveau exposé au pouvoir de l'algorithme. Cette tactique technique n'a en quelque sorte pas réussi à triompher au sein du collectif.

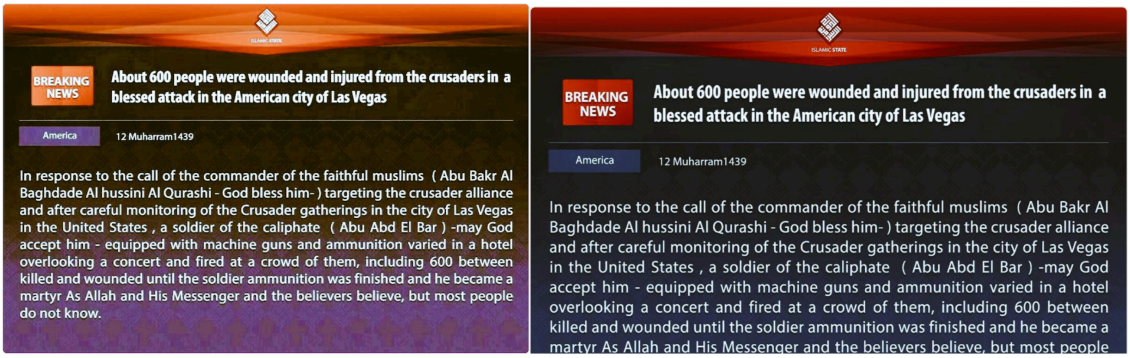

Figure 8.2. Exemple d'un contenu altéré. Il s'agit ici du communiqué officiel de l'État islamique concernant l'attaque à Las Vegas s'étant déroulée le 1er octobre 2017. À gauche le contenu altéré, à droite le contenu non altéré. Ici, les pixels de l'image ont simplement été réduits.

8.2.2. Créer des comptes et des chaînes réservistes

> Terror (Forwaded messages): If this channel goes down i am taking a break
>
> LL 10//
> Don't akhi
> I have several back ups for you to utilized
> (Chaîne Telegram, 24 juillet 2017)

L'échange ci-dessus témoigne d'une tactique qui consiste à créer et échanger des comptes et des chaînes « réservistes ». De la sorte, certains militants se sont transformés en d'importants producteurs de comptes de réseaux sociaux et de chaînes « back up ». Des partisans ont toutefois été tentés de mettre en place des formes d'organisation plus formelles dont le seul objectif est de constituer des banques d'approvisionnement de comptes de réseaux sociaux. En d'autres termes, ces collectifs ont spécifiquement pour but de ravitailler les troupes en comptes de réseaux sociaux afin que le flux informationnel ne soit jamais dans le dénuement. En effet, en proposant des comptes « prêts à l'emploi » aux utilisateurs, ils les déchargent des contraintes de l'ouverture de nouveaux comptes et leur permettent de réacheminer rapidement le flux informationnel. Cette gamme de service peut aussi s'élargir à une banque de numéros pour confirmer les comptes de réseaux sociaux.

Cette mission est attribuable à plusieurs collectifs anonymes qui publicisent leur action sur Telegram. Pour donner crédit au sérieux de cette opération, s'affirme pour ces derniers la nécessité de créer une identité avec un nom et un logo. Leur action est, d'une façon très explicite, le miroir d'un professionnalisme et d'un acte offensif. Certains se décrivent comme des brigades qui saisissent d'importants butins en pillant l'ennemi de comptes dormants. Simultanément, elles tirent parti du terrain en créant une panoplie de nouveaux comptes. Afin

d'attester de leurs opérations, les collectifs ne manquent pas de produire des bilans de leurs résultats, tant il est important de signifier leur tour de force.

Ces résultats sont toutefois très inégalitaires selon les collectifs. Les plus efficaces se targuaient d'avoir une banque d'approvisionnement qui atteignait plusieurs milliers de comptes en seulement un mois. En revanche, d'autres collectifs, n'atteignaient le millier qu'après plusieurs mois. Dans la plupart des cas, les comptes Twitter constituent la plus grande quantité du butin. Les écarts entre le nombre de comptes Twitter et Facebook peuvent d'ailleurs être extrêmement importants. Pour éviter que ces comptes « prêts à l'emploi » ne tombent dans les mains de l'ennemi, certains collectifs ont trouvé bon de demander des preuves supplémentaires aux utilisateurs souhaitant en acquérir. Ils veulent être en contrôle dans un environnement où l'anonymat prévaut. Aucune duperie n'est tolérée. Il arrivait alors qu'il soit demandé à l'internaute de fournir des captures d'écran de leurs publications sur d'autres réseaux sociaux qui attestent de leur soutien à l'État islamique.

Ces collectifs sont une part du tour de force. En réalité, sur Telegram, les internautes produisent de nombreuses chaînes « miroirs » ou « réservistes ». Aucun service spécialisé ne prévoyait des chaînes « prêtes à l'emploi », pour la simple et bonne raison que Telegram ne restreint pas le nombre de fois qu'un internaute puisse créer une chaîne ou un groupe. Les partisans sont ainsi à même de pouvoir gérer individuellement leur propre banque d'approvisionnement. C'est ainsi que par exemple certaines chaînes très influentes sur Telegram, affirmaient exploiter 300 chaînes et groupes en même temps. Un chiffre qui est monté jusqu'à 600 trois mois plus tard. Sans doute quelque peu exagéré, il n'en demeure pas moins que lors de notre enquête le groupe en question possédait un grand nombre de chaînes et de groupes actifs en même temps. Une tactique payante en ce qu'elle a l'avantage d'atténuer l'impact des suspensions. Malgré les suspensions, les centaines de chaînes et de groupes en activités permettent d'assurer le relais. Au-delà, ces opérations communiquent sur deux versants : celui de la victoire et celui de la lutte. En communiquant sur ces stratégies, ils font éclater en plein jour une manifestation de force : celle d'une capture et d'une profusion de comptes de réseaux sociaux, redoutable pour que le flux informationnel ne soit jamais tari par la modération.

Figure 8.3 Exemple d'infographie faisant état du bilan opérationnel d'une brigade. Elle a été distribuée en plusieurs langues sur Telegram en avril 2018.

8.2.3. Fabriquer des chaînes de solidarité

Dans un contexte où le collectif est quotidiennement la cible de suspensions, la solidarité entre les partisans s'est rapidement instaurée. Ils ont développé des mécanismes promotionnels d'envergure pour propager les nouvelles chaînes et groupes Telegram et les comptes de réseaux sociaux. Cette efficacité ne saurait s'exécuter sans l'aide d'un artefact technique ; celui de la fonctionnalité de partage. Il se présente comme une fonctionnalité d'usage et fait pleinement partie de l'environnement numérique à travers lequel les utilisateurs naviguent. Il permet une opération simple et rapide qui nécessite peu de connaissances techniques. Ces agencements tangibles dans le monde des technologies de l'information, ont permis au collectif d'amplifier et de rendre visible la réapparition de ses militants. La solidarité s'exécute ainsi à travers une chaîne de médiation complexe, que nous allons décrire à partir du cas précis de Telegram.

Une brève mise en contexte s'impose dans un premier temps. Pour rejoindre un groupe sur Telegram, deux options s'offrent à l'utilisateur : passer par un lien d'invitation ou par la fonction de recherche de Telegram. C'est la première option que les partisans de l'État islamique ont privilégiée. L'avantage pour ces derniers est qu'ils peuvent attribuer un temps de validité au lien d'invitation, rendant l'accès plus difficile pour ses adversaires. Un temps de validité souvent court, oscillant entre une trentaine de minutes ou quelques heures.

> Nouveau lien pour rejoindre le channel disponible 1 à 2 heures seulement. Lien : https://t.me/joinchat/---- #Partagez #Rejoignez. (Publication groupe Telegram, 17 juillet 2017)

Reste que pour qu'un certain nombre de militants puisse avoir accès à la chaîne, il lui faudra être largement publicisée. Dans le cours du fonctionnement, cela se manifeste par le guidage de conduites suggérées qui se traduisent par des formules simples comme « join and spread ». Elles prescrivent un geste exemplaire à poursuivre pour le collectif. La chaîne de solidarité commence ainsi : elle met de proche en proche des humains avec une fonctionnalité informatique. Cette dernière assure a priori le lien de la solidarité entre la nouvelle chaîne à publiciser et les autres utilisateurs. Les utilisateurs ne sont effectivement nullement obligés de se conformer à une telle exigence. Le fonctionnement de l'alignement entre ces êtres n'a franchement pas toujours été victorieux. C'est une incertitude que chaque auteur de nouvelle chaîne doit assumer. En fait, le succès de publicisation d'une nouvelle chaîne dépend du succès de la précédente. En quelque sorte, une mémoire collective se forme autour des chaînes qui méritent l'attention ou non. La fonctionnalité informatique de partage est ainsi très différente de la fonction de mémoire et de perception de l'humain qui accrédite l'importance d'une chaîne. C'est donc de la synergie de ces deux êtres que chaque nouvelle chaîne retrouvera une place rapide dans le réseau.

Si dans ce qui précède, nous avons essentiellement souligné le rôle des humains dans la publicisation des nouvelles chaînes Telegram, les *botnets* sont également solidaires de l'action. Ces derniers ont permis la distribution automatique de nombreux liens d'invitation. Dans ce schéma automatisé, l'acte de publicisation est plus rapide, mais aussi plus épuré. Comparons rapidement. Dans les cas où la publicisation découlait de l'humain, un texte était généralement joint aux nouveaux liens. On pouvait y lire par exemple une courte introduction, les objectifs et dans certains cas le règlement de la chaîne ou du groupe[121].

> We are delighted to annouce the launch of our channel which provides the latest news, events, and statements on the Islamic State and our beloved Ummah.
>
> Kindly join our public channel and stay up to date with the latest news as they happen. https://t.me/---

[121] Ces règles sont multiples et de différents ordres. Elles concernent les groupes Telegram, puisque ces dernières permettent à tous les internautes d'interagir. Par exemple, on peut trouver des règles qui imposent de parler l'anglais, d'être respectueux envers les autres, de publier des autocollants et des GIFS avec parcimonie, de ne pas *spammer*, de faire des publications pertinentes ou encore d'interdire l'accès aux femmes.

> Please join, support, and publicize the channel. (Groupe Telegram, 19 octobre 2017

Dans le cas des *botnets*, la mise en forme est plus impersonnelle. On y voyait la photo de profil et le nom de la chaîne. À la suite de quoi, deux options se déroulaient : « join it » et « share it ». Un moyen efficace qui permet de rejoindre et de répandre la nouvelle chaîne par un simple bouton.

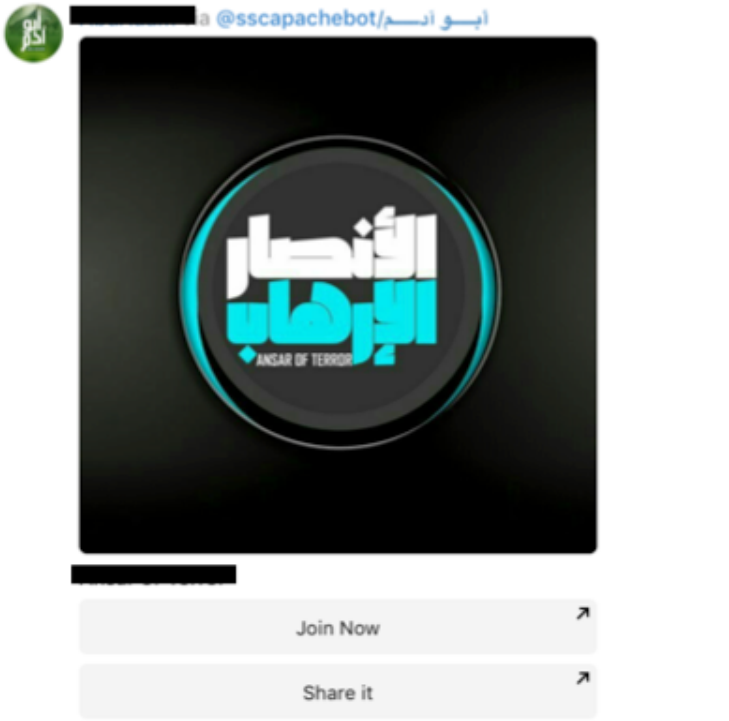

Figure 8.4. Exemple d'un utilisateur qui a partagé la nouvelle chaîne via le *botnet* sscapachebot le 20 octobre 2017.

On remarque ainsi une variabilité dans les mises en scène des nouvelles chaînes selon qu'elles sont traitées par des partisans ou des *botnets*. Il n'est pas question de les hiérarchiser, mais de montrer comment la publicisation de celles-ci fonctionne dans des relations d'interconnexion entre différentes individualités. En somme, la publicisation se couple à des humains et à des machines, lui corrélant un ensemble de formats.

Reste une dernière variabilité : la mise en place d'un dispositif de régulation et de règlements de la distribution. Cette régulation assumée par l'humain donne une direction précise et stricte du partage des liens d'invitation. Dans certains cas nous pouvions lire :

- Don’t should be shared on Twitter nor Facebook
- Don’t share on groups
- Join and share to the trusted ones ONLY !!!

Cette régulation absorbe en elle un problème majeur auquel fait face le collectif : les risques d’espionnage[122]. Si l’espionnage n’a pas attendu les technologies numériques pour exister et fait partie de l’arsenal militaire et politique depuis des millénaires (Gergorin et Isaac-Dognin, 2018), cette activité s’en trouve néanmoins facilitée et plus accessible grâce aux innovations technologiques. Au sein du collectif, la sanction de comportements suspicieux et hors-norme est immédiate et abrupte :

> Any person displaying suspicious behavior or creating trouble will be removed (Effective Immediately) by the admins. Rafida and troublemakers will be removed without hesitation. This group is strictly monitored and administered by dedicated munasireen. (Groupe Telegram, 20 août 2017)

En cela, l’humain assure la régulation du fonctionnement de partage. Il est celui qui connaît les problématiques internes à la visibilité et qui cherche à réduire leur occurrence. Pour reprendre Simondon (1958) « les machines au contraire ignorent les solutions générales, ne peuvent résoudre de problèmes généraux » (p.176). Cela ne veut pas dire qu’elles ne s’impliquent dans aucune activité de régulation. Mais, toutes les fois qu’il a été possible de les observer dans ce type de rôle, elles réalisaient des opérations simples.

Pour être complet, considérons une dernière ligne d’évolution de cette solidarité. Le point que nous voulons souligner ici est la mise en place de dispositifs de centralisation des nouveaux liens. Au sein du collectif, cela signifie de créer des chaînes dédiées spécifiquement à la distribution de liens d’invitation. Elles agissent comme des instruments de stockage qui opèrent une distribution plus coordonnée. Trois rôles ressortent ainsi de ces chaînes : mettre à disposition une interface qui regroupe les liens d’invitation ; repérer et collecter ces nouveaux liens ; et enfin, fournir la possibilité aux militants de rejoindre facilement les nouvelles chaînes. Par ces mécanismes qui permettent la publicisation de nouveaux liens, nous pouvions

[122] Au sein de l’islam, l’espionnage est considéré comme un péché majeur et est explicitement interdit dans le Coran (Maher, 2016). L’espionnage est lié à l’idée de médisance et est comparé au fait de manger la chair d’un frère mort (Coran 49 :12). L’espionnage cause notamment la discorde en propageant la suspicion et les querelles (f*itna*). Au sein des mouvances jihadistes, l’espionnage est toujours assimilé à la fois à l’apostasie et à l’hostilité inhérente envers les musulmans.

facilement rejoindre des dizaines de chaînes par jour. Ainsi, nous avions toujours accès aux dernières diffusions et contenus de l'État islamique, et ce malgré des suspensions toujours plus fréquentes sur Telegram.

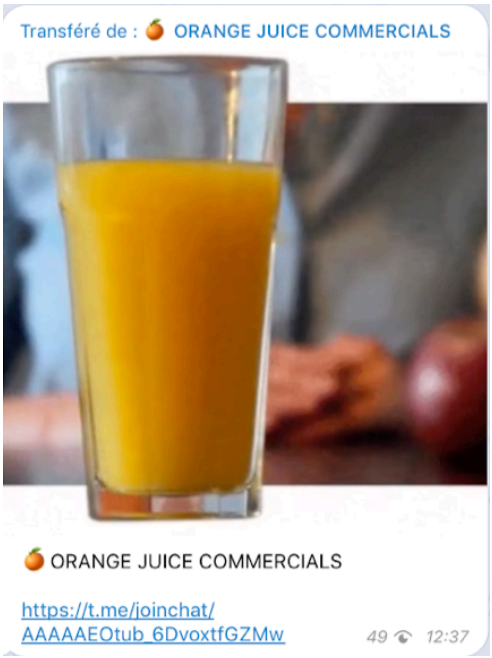

Figure 8.5. Lien d'invitation pour une chaîne distributrice de nouvelles chaînes pro État islamique active en mars 2018. En apparence, rien ne peut indiquer à l'internaute qui voudrait rejoindre le lien d'invitation qu'il s'agit d'une chaîne pro État islamique. Si les noms de ces chaînes pouvaient être explicites (par exemple Links ou LinksUpChannel), elles pouvaient également être implicites comme ci-dessus, pour duper les internautes malveillants envers l'État islamique.

8.2.4. Archiver les contenus

Résister à la modération exige de mettre en place un système d'archivage. Si le contenu est supprimé d'une plateforme, il doit pouvoir réapparaître. C'est en ce sens que le collectif a entrepris de télécharger et d'archiver ses contenus. Dans cet esprit, certaines chaînes suggéraient aux militants d'entreprendre des sauvegardes du matériel distribué :

> Important. Make a clone channel and start copying all the ressources to save before kuffar delete the channel again. We've got more posts remaining. (Chaîne Telegram, 13 avril 2017)

La raison de cette activité est donc claire : faire survivre les énoncés. Le collectif passait maître dans l'art de répartir les contenus sur différentes plateformes. Une tactique fortement utilisée lors de l'apparition de nouvelles productions de l'État islamique. Ces dernières, lorsque publiées sur Telegram, pouvaient contenir pas moins de 60 liens externes hébergeant et stockant les contenus. Une pratique qui peut se renouveler pour redistribuer d'anciens

contenus officiels de l'État islamique. Chaque production de l'État islamique garde ainsi la possibilité de reparaître en tout temps et de multiple fois. Ainsi, le collectif établit des connexions entre des plateformes. Il joue avec l'immédiat et l'archive (Gehl, 2014).

Pour constituer la base de son opération, le collectif utilise de nombreux types de plateformes. Sites d'archivage, de partages et de téléchargement de vidéos, Cloud forment l'arsenal d'un archivage réussi. On y trouve les grandes plateformes comme Amazon Drive, Google Drive, Dropox et YouTube. Mais aussi de multiples plateformes plus petites et plus ardues à réguler en matière de modération. Cette tactique devient capitale pour assurer la flexibilité et la disponibilité des contenus. Toutes les plateformes ne disposent pas des mêmes capacités de modération que les grandes plateformes numériques. La durée de vie d'un contenu diffère d'une plateforme à l'autre. En aménageant un tel système de distribution le collectif assure la pérennité de ses contenus : si un contenu est supprimé d'une plateforme, il reste accessible sur une autre. Par ailleurs, ceci manifeste un assouplissement considérable des modalités de distribution des contenus. Ces liens sont effectivement facilement transposables d'une plateforme à une autre en les copiant-collants.

Nous pouvons noter que cette tendance à la répartition distribuée des contenus se développe comme une réponse à des dispositifs techniques incertains et changeants. Cette flexibilité émane ainsi d'une incertitude, qui ne leur permet plus de compter sur une stabilité du dispositif technique. Pour cela, il doit continuellement explorer d'autres plateformes pour sécuriser son contenu. Cette tactique permet essentiellement de miser sur la durabilité de l'information, plus que sur la possibilité d'atteindre une large audience. L'expérience de l'État islamique nous apprend donc une chose sur la modération : cette dernière n'a pas pour effet d'annihiler la propagande de l'État islamique, plus que de la morceler et de la fragmenter au sein d'une série de plateformes plus difficile à contrôler.

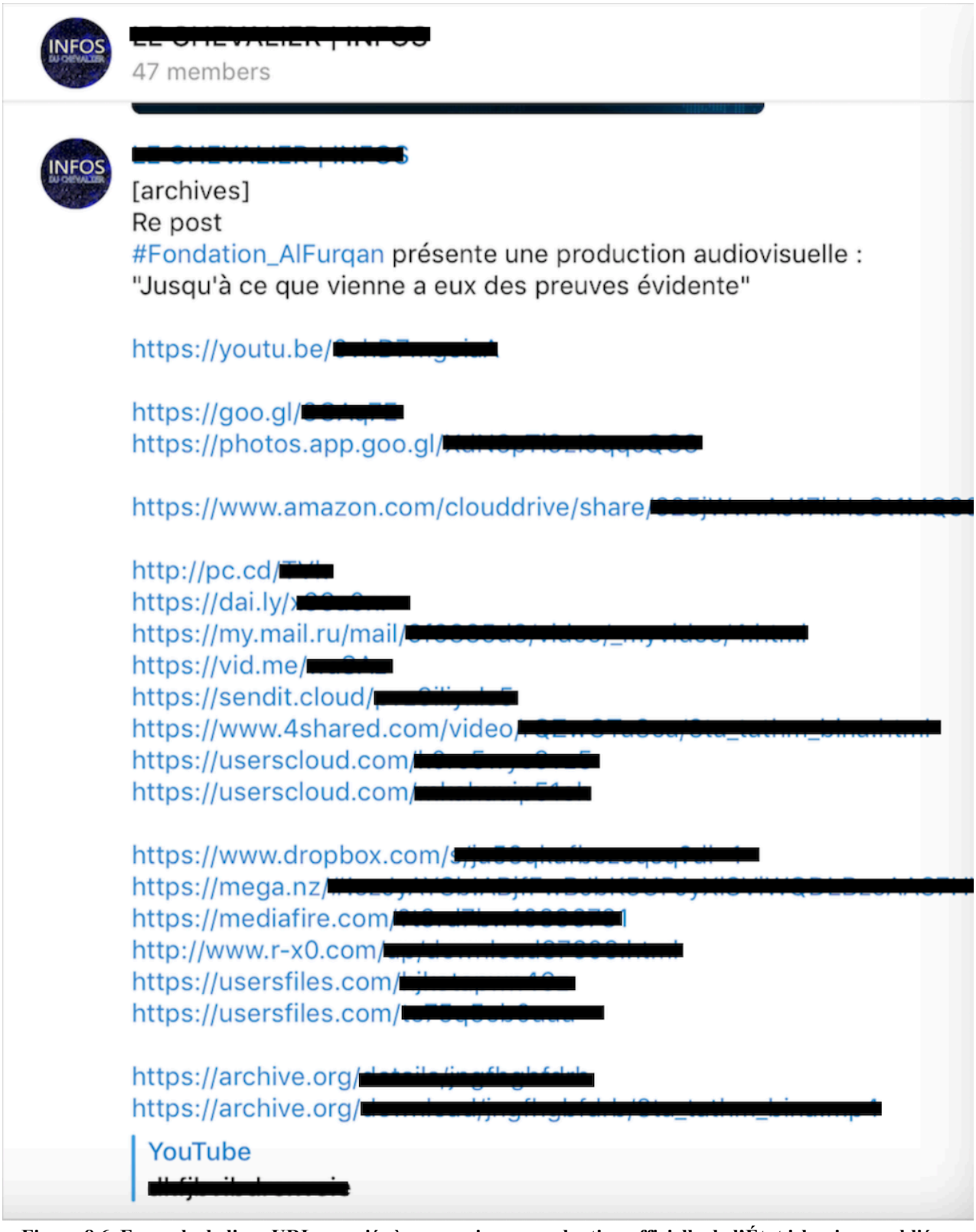

Figure 8.6. Exemple de liens URL associés à une ancienne production officielle de l'État islamique publié sur Telegram le 26 octobre 2017.

8.2.5. Migrer vers d'autres plateformes

Baaz, Viber, Ask.fm, Kik, Threema, Riot.im, Rocket chat, ZeroNet. Ce sont là quelques exemples de plateformes numériques que le collectif a cherchées à s'approprier en parallèle des grandes plateformes numériques et à Telegram. Ainsi, la reconnaissance du morcellement et de la fragmentation évoqués ci-dessus ne s'arrête pas aux seules plateformes d'archivage. Elle forme un principe général de mobilité du collectif pour permette au « voir » de perdurer, face à une modération toujours plus tenace. C'était déjà le cas en 2015. Lorsque Twitter a renforcé sa politique de modération, les partisans ont trouvé en Telegram un nouveau terreau pour propager et organiser leur propagande. C'est en cela que face à la modération, on peut observer la mise au point de « pratiques d'espace » (De Certeau, 1990) qui organisent des mouvements et des déplacements vers d'autres plateformes. La chaîne de visibilité s'allonge, mais devient par là instable. Elle s'allonge, car migrer ne signifie pas l'abandon des réseaux sociaux traditionnels. À cet égard, le collectif effectue des appels récurrents qui incitent les militants à poursuivre la tâche d'envahissement sur les principales plateformes de réseaux sociaux. Elle est instable, car elle ne garantit pas que la nouvelle plateforme exploitée soit un succès.

Prenons le cas de la plateforme de réseaux sociaux Baaz. Le collectif a commencé à promouvoir sa propagande sur ce réseau en juin 2017. Ce réseau social basé à San Francisco a été créé en 2015. Il se décrit comme un réseau social de nouvelle génération, conçu pour un public multinational : « Baaz is a truly global company expanding the reach of social media in underserved markets »[123]. La particularité de Baaz est qu'il délivre « a unique mix of social aggregation, trending stories, messaging and general social networking ». Il agit comme un agrégateur des médias sociaux en connectant le profil de l'utilisateur à plus de 150 réseaux sociaux. Le réseau prend actuellement en charge les langes anglais et arabes. Comme il est maintenant coutume de l'observer, les militants ont fait de Telegram une ressource clé pour publiciser l'usage de nouvelles plateformes et relayer les liens URL.

[123] Voir le site web de la plateforme : https://help.baaz.com/knowledgebase/articles/1100098-how-is-baaz-different-from-other-social-networks

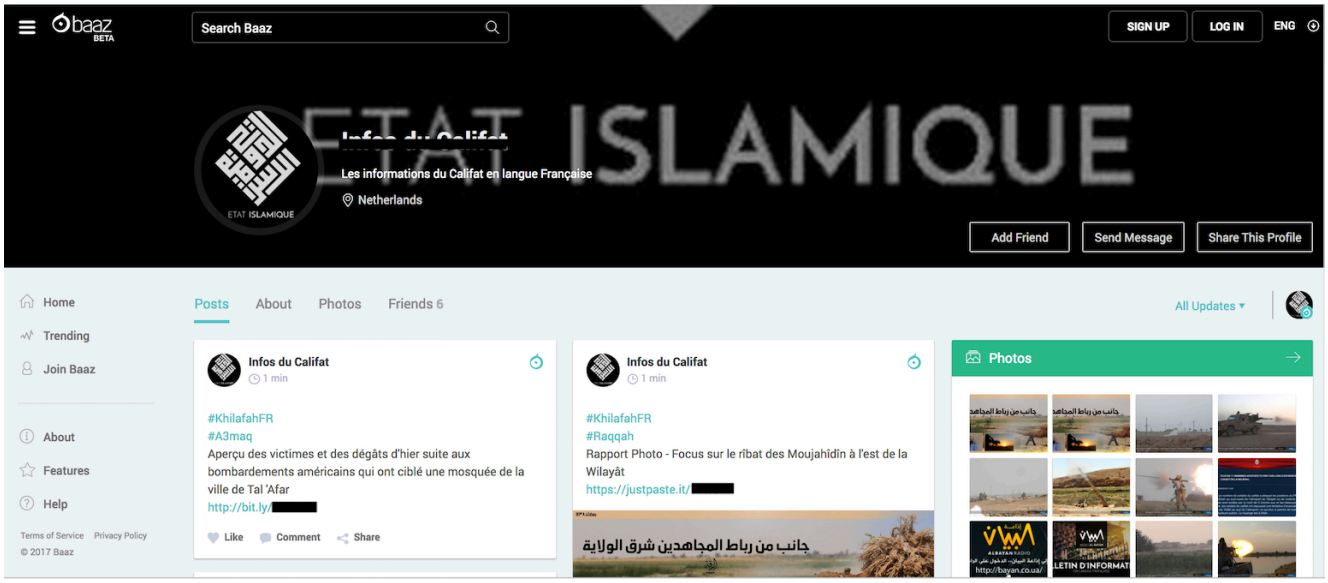

Figure 8.7. Exemple d'une interface d'un partisan de l'État islamique sur Baaz en date du 15 juin 2017.

Ce type de plateforme, encore jeune dans son développement, suppose des dispositifs de modération moins puissants que les grandes plateformes numériques. Une caractéristique de prime abord avantageuse pour le collectif. Il n'en demeure pas moins que la plateforme modère. Et qui plus est, elle a très vite fait de renforcer sa modération pour exclure le collectif de la plateforme.

> If the content contains any offensive or know Jihadi content we act immediately. Our policy and position is unequivocal, and we do not tolerate, condone, support or accept such content[124].

La réalité de son destin a donc rapidement rattrapé le collectif : tout comme sur les autres plateformes, sa propagande allait à nouveau connaître de lourdes interférences. Faible succès d'audience et modération ont finalement poussé le collectif à abandonner la plateforme quelques semaines plus tard.

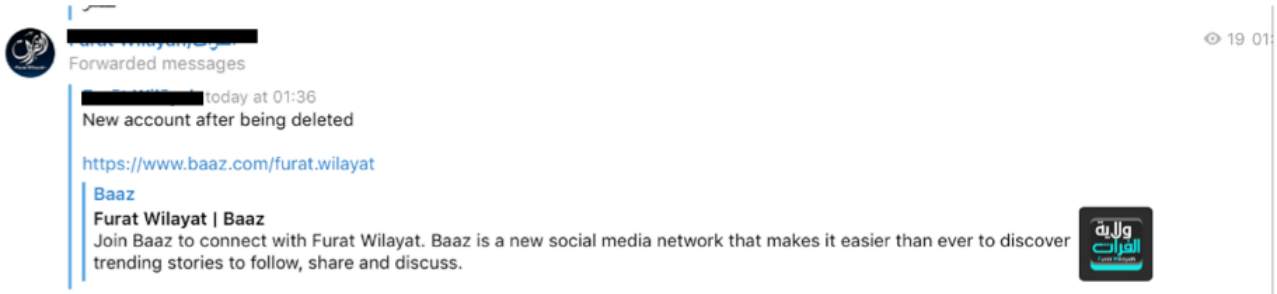

Figure 8.8. Redistribution d'un nouveau lien Baaz après suspension. Message publié sur Telegram le 14 juin 2017.

[124] Porte-parole du réseau Baaz, entrevue donnée à la BBC, 12 juin 2017. Voir : https://www.bbc.com/news/technology-40246763

Terminons par un autre exemple non négligeable. Pour échapper à la modération, le collectif a également misé sur le web décentralisé[125]. Lors de notre enquête, des liens vers la plateforme Riot.im ainsi que des tutoriels sur son utilisation ont de plus de plus en plus été diffusés sur Telegram. Riot.im est une plateforme de diffusion décentralisée et cryptée basée sur le protocole Matrix. La plateforme se décrit comme une « universal secure chat app entirely under your control ». Sur le site de la plateforme, nous n'avons pas trouvé de conditions d'utilisation, mais un manifeste qui fait l'éloge de la liberté d'expression :

> Our manifesto
> We believe that people should have full control over their own communication.
> We believe the ability to converse securely and privately is a basic human right.
> We believe that communication should be available to everyone as a free and open, unencumbered, standard and global network.
> We believe in freedom.

Face au fait que l'État islamique exploite leur plateforme, ces derniers ont dû se résoudre à intégrer un plan de modération pour limiter la propagation de cet usager indésirable. Nous avons ainsi été maintes fois heurtés à des pages dont le contenu avait été suspendu.

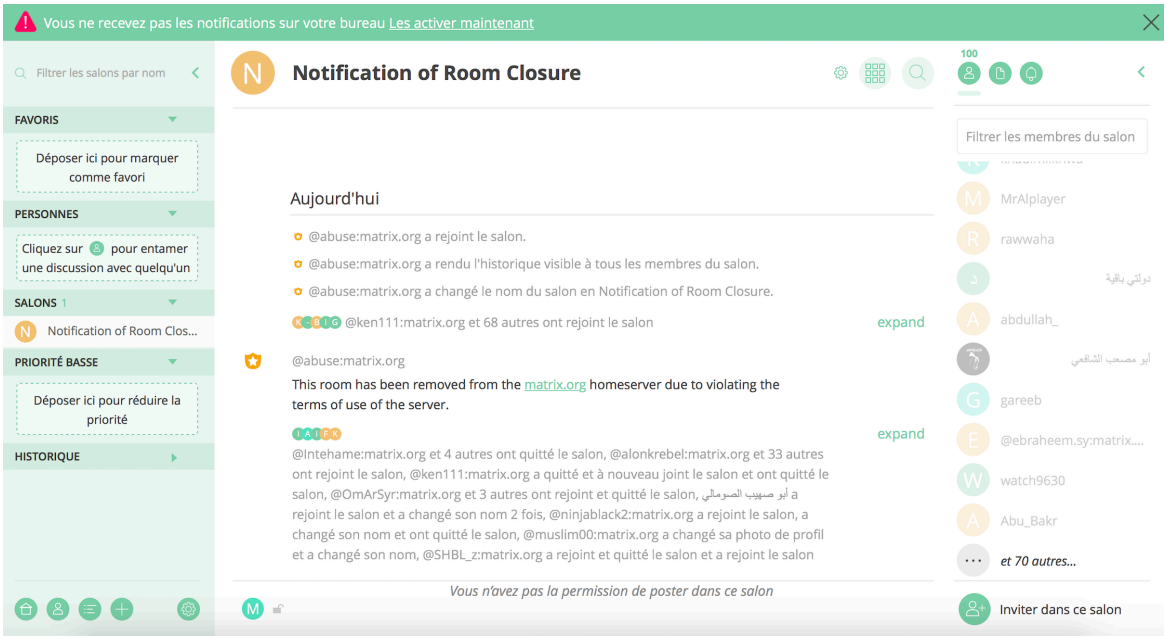

Figure 8.9. Notification de la suppression du salon en raison d'une violation des termes du service en septembre 2017.

[125] Le web décentralisé repose sur le modèle pair-à-pair (P2P). Il s'agit d'un « modèle de réseau informatique structuré de manière décentralisée, afin que les communications ou les échanges qui y ont lieu se fassent entre nœuds dotés d'une responsabilité égale dans le système » (Musiani, 2015 :47).

Ces exemples nous apprennent qu'en migrant vers des architectures et des réseaux sociaux différents, le collectif marque sa détermination à perdurer dans l'écosystème numérique. Il est perpétuellement à la recherche de nouvelles plateformes qui lui permettent d'acquérir visibilité, stabilité et sécurité. Ce principe de migration exige par conséquent une souplesse maximale de la part du collectif. Il suppose des systèmes de repérages rapides. En quelque sorte, il doit perpétuellement rester attentif aux diverses plateformes disponibles sur le web.

Nous pouvons conclure que le collectif évolue par ce fait dans un contexte où les repères de visibilité se multiplient et se juxtaposent. De là, émerge une incertitude : combien de temps perdurera le collectif sur la plateforme ? Quelle sera la prochaine plateforme de prédilection ? Nous l'avons vu, à l'exception de Telegram, les autres essais d'appropriation de nouvelles plateformes se sont soldés par de courts passages, des tentatives infructueuses et des échecs. Rien ne garantit une appropriation réussie du collectif. On comprend ainsi que l'une des caractéristiques d'un tel mouvement est de renflouer la variabilité des repères, tout en renforçant l'incertitude et l'instabilité. En revanche, les mouvements de migration se font davantage vers de plus petites plateformes et des espaces plus clos, ce qui rend la force du contrôle plus difficile. Ce morcellement des plateformes agit ainsi comme une possibilité d'agencement par lequel l'État islamique se maintient en ligne et assure sa visibilité.

8.3. Étude de cas : Asma compte martyre par excellence

En dépit de la modération sur Twitter, bon nombre d'utilisateurs ont été capables de revenir sur la plateforme avec des comptes explicitement pro État islamique. Dans cette section, nous partirons du cas particulier d'Asma. Comme pour les autres internautes nous ne détenons pas d'informations sur cet utilisateur, mis à part qu'elle se présente comme étant une femme. Cette internaute est une revenante expérimentée. Elle est connue tant dans la sphère jihadiste qu'auprès des « traqueurs » de jihadistes. Lors de notre enquête, elle est réapparue une centaine de fois. Chaque profil d'Asma que nous avons observé jouait la même carte de l'authenticité. Le camouflage n'était pas une option pour cette internaute. La vérité de son appartenance à l'État islamique devait éclater au grand jour.

Arborant un style résolument pro État islamique, elle a habitué son observateur et son spectateur à la constance. Au fil des suspensions, elle utilisait toujours le même pseudonyme. L'esthétique de son profil faisait quant à lui état d'une grande stabilité. Roses, étendard de

l'État islamique, combattants de l'État islamique victorieux ou encore mis en scène dans de longues chaînes de pick-up formaient son répertoire pictural de photos de profil et de bannière. Pour incarner avec plus de vigueur cette identité pro État islamique, Asma distribuait du contenu officiel et non officiel de l'État islamique, en passant par l'accentuation hyperbolique des éléments ouvertement menaçants et violents. Elle publicisait les nouvelles productions, tout en choisissant les mèmes les plus virulents. Les publications d'Asma contenaient tous les ingrédients qui tôt ou tard justifieraient son exclusion : apologie du terrorisme, célébration des attentats, menaces explicites envers ses adversaires, etc.

Asma sait très bien qu'il faudra peu de temps pour que son compte soit suspendu. Mais peu importe qu'il soit supprimé en quelques minutes ou quelques heures. Pour l'internaute, il s'agissait de faire la démonstration de son aptitude à revenir sur la plateforme qui l'exclut. Et cette capacité, elle savait la manier dans des délais extrêmement brefs. Il était commun d'observer qu'en une heure Asma était à son deuxième compte. C'est un art de réapparaître. Asma manie des coups de ruse ; elle manipule le dispositif technique ; elle produit une évidence au public qu'elle vise, c'est-à-dire les failles de la modération et l'ingéniosité dont elle fait preuve.

Cet art prend effet s'il est rendu visible. En d'autres termes, s'il est soutenu par les autres militants. Auquel cas, le compte se mue dans une invisibilité et une indifférence sans borne. Comme nous l'avons dit plus haut, Asma bénéficiait d'une grande popularité au sein du réseau. Ainsi, un nouveau compte de Asma suscitait l'attention des autres militants qui ne manquaient pas de le publiciser et de le médiatiser. Le profil devenait un point voyant. Bien entendu, simultanément, l'internaute reconstituait son réseau d'abonnements[126], ce qui d'une certaine manière lui permettait de signaler son propre retour aux autres internautes pro État islamique.

S'efface donc l'idéal d'une modération effective qui annihilerait la présence de l'État islamique. Et cette faille, le collectif a bien l'attention de l'afficher en réapparaissant perpétuellement malgré les suspensions. Pire, il ne cherche même pas à modifier leur profil

[126] Face aux modérations répétées, le nombre d'abonnés et d'abonnements moyens des partisans de l'État islamique a drastiquement chuté. Entre septembre et décembre 2014, l'étude de Berger et Morgan (2014) montre que le nombre moyen d'abonnés était de 1004, contre 208 pour tout autre utilisateur actif. En moyenne, le nombre d'abonnés d'Asma ne dépassait pas la barre des 25. Le maximum d'abonnés atteint par Asma a été une fois de 120. Les suspensions montrent ainsi qu'elles peuvent avoir un effet néfaste pour le collectif.

malgré les avertissements. Il réplique le même style de comptes au fil des suspensions. Cette propension de « compte martyre » - c'est-à-dire aménagé de façon à ce qu'il n'échappe pas à la modération- est volontairement mise en exergue pour signifier à ses adversaires qu'ils ont l'avantage sur la plateforme. Ces actes donnent la preuve qu'ils manient avec habileté la plateforme, et ce sans doute mieux que d'autres utilisateurs actifs.

8.4. Étude de cas : La duperie comme mode d'action

Time Magazine. Reuters World. Apple Store. McDonald's. Pavel Dourov. Yes we can. BBC Arabic. Voici un ensemble de slogans, de marques, d'agences de presse et de personnalités publiques que les militants de l'État islamique se sont appropriés pour nommer leurs nouvelles chaînes Telegram ou profil de réseaux sociaux. Ce détournement s'exerce par les opérations suivantes : réappropriation de logos et de codes de l'entité médiatique et commerciale visée. Dans le cas d'une personne, il s'agit de reprendre sa photo. Une fois le détournement opéré, les militants distribuent le matériel pro État islamique à profusion.

On peut y voir un acte qui vise à passer sous les radars. Bien que la duperie soit de courte durée, puisque les contenus de la chaîne ou du profil étaient explicitement pro État islamique. Sinon, on peut y voir simplement un acte d'amusement et de provocation. Parfois, cela leur permettait de produire des canulars qui ironisaient sur leur condition d'internaute à exclure. Sur la fausse chaîne Pavel Dourov, cofondateur de Telegram, créé par des militants de l'État islamique, on pouvait lire :

> There was some mistake in system which resulted in my suspension. I'm back again to keep you all updated thanks for sticking with me
> Pavel Durov,
> Creator and CEO of Telegram and VK (Chaîne Telegram, 14 septembre 2017)

Par ces détournements, les jihadistes expriment qu'ils connaissant très bien le monde qui les entoure. Dans cette manœuvre du *lointain* et du *proche*, du *eux* et du *nous*, elle introduit la pratique de la satire et de la parodie. Ils sélectionnent donc. Et ils sélectionnent explicitement des grands emblèmes de la société qu'ils combattent. Ce faisant, cette duperie est moins insidieuse que dans le cas de vol d'identités en ligne. Elle cherche à créer du discontinu dans son identité militante en s'emparant d'un nouveau masque. Une discontinuité qui se veut temporaire, partielle et voulue. Il tente une nouvelle voie en simulant « à semi » un autre. Un

autre qui n'est rien d'autre que la société qu'il condamne. Quelle ironie que de voir une chaîne nommée Time Magazine publier du contenu de l'État islamique.

Cette série de tours et détours qui leur permet de combiner des identités différentes renvoie à une potentialité offerte par les technologies du web. Quelques clics suffisent pour aller chercher les informations en ligne et les assembler. Par ailleurs, si les utilisateurs sont libres de choisir les noms et les pseudonymes qu'ils souhaitent sur Telegram et Twitter, usurper l'identité d'un utilisateur est prohibée par celles-ci. Plutôt que s'attaquer aux individus, il pénètre néanmoins de grands emblèmes occidentaux et capitalistes. Quoique cette tactique de duperie ne soit pas spécialement prolifique au sein des partisans, il n'en demeure pas moins qu'elle révèle que le collectif peut être très imaginatif pour se mettre en scène. Rappelons que la simulation de l'identité militante dans la première étude de cas valorise celle d'une présentation de soi purement partisane. Ici, le scénario est cette fois-ci autre. Il y insinue la multitude en jouant avec des identités opposées. Le collectif performe ainsi sa narration à partir d'une interface qui se veut moins explicite. Il manœuvre l'illusion. Il crée le divertissement.

Conclusion : Visibilité et résistance

Le chapitre 7 nous a montré qu'au sein du web tout le monde n'a pas le même droit de parole : les contenus radicaux sont modérés. Les descriptions et analyses de ce dernier chapitre dévoilent que le collectif contourne cette censure avec un succès mesuré. Dans cette dynamique, il ne s'agit plus seulement pour le collectif de diffuser leur matériel médiatique, mais de lutter pour rester visible. La performativité de la visibilité du collectif change maintenant de cap. Elle nécessite d'aligner une série d'intermédiaires et de traductions successives qui lui permettront de résister à la modération.

En cela, la modération bouleverse la coordination entre le dispositif technique et le collectif. Elle le place dans une incertitude. Elle lui impose l'instabilité. Elle lui ordonne la discipline. C'est ici que s'articule le point de basculement. Nos analyses démontrent que le collectif refuse l'assujettissement. Il conteste la place « d'utilisateur à exclure » que les plateformes numériques lui imposent. Il cherche à la combattre de manière immédiate. De là, le collectif introduit un nouveau modèle d'articulation : celui de la désobéissance. Il resurgit sur le champ de l'affrontement, mais d'une manière différente que celui décrit dans le chapitre 5 et 6. Cette

fois-ci, il se situe dans l'ordre de la protestation contre les alliances faites par le dispositif technique qui vise à le déloger de l'espace. Ce n'est plus seulement le collectif qui mène le combat. Il doit maintenant organiser sa visibilité dans un environnement qui lui est extrêmement hostile. Et à travers cette réalité, nous avons exposé que le collectif se défend. Il devient un habile bricoleur et tacticien qui cherche des solutions pour que sa propagande continue à circuler. Ainsi, ce qu'on voit, c'est que la modération mène à des tactiques d'évitement plus qu'à une résignation.

Ce chapitre nous a permis de découvrir les points d'application et les méthodes de ces tactiques. Le collectif organise des solidarités, des transgressions, des manipulations et des mobilités. Cela traduit un ensemble de tactiques prenant corps dans l'environnement même des technologies du web. Les technologies du web offrent ainsi au collectif les possibilités de la réalisation de sa lutte. Partout, dans chacune des tactiques, c'est l'agencement même qui constitue le système de lutte. Créer des comptes réservistes, n'existe que par un agencement humain – non-humain. Transgresser l'algorithme entraîne un autre type d'agencement humain – non-humain. En somme, la nature des agencements varie et n'a pas les mêmes effets. Ils mélangent différents styles organisationnels, de solidarités et d'agentivité humaines et non-humaines.

Cela étant dit, il faut préciser les éléments de langage qui accréditent ces tactiques de résistance. Le collectif ne met pas seulement en œuvre des tactiques et des solutions. Il sort de sa condition de bricoleur et de tacticien pour constituer un dire sur ses exclusions. Il informe son adversaire de ses retours. Il communique sur son sort. Parfois, il ironise, parfois il le condamne. L'intérêt de cette rhétorique est d'attirer d'abord l'attention sur les failles du dispositif de contrôle des plateformes numériques. Le collectif se veut être la preuve que les plateformes numériques sont inaptes à la régulation. Il ne cherche en rien à communiquer avec l'adversaire ; mais bien de l'informer que ses efforts sont vains.

Au fond, tout cela montre l'incapacité de la firme propriétaire à « discipliner l'utilisation » (Thévenot, 1993). L'usager est capable de se reconfigurer dans des nouveaux usages qui créent les possibilités de ripostes inattendues. Il joue avec les règles. Il les transgresse aussi. Est-ce dire que l'usager occupe une position de toute-puissance face au dispositif technique ? Certainement pas. Il faut dire que si les techniques de modération amènent à mettre en place des tactiques d'évitement chez les internautes, ces dernières ont la capacité de désorganiser la

visibilité et de la rendre plus contraignante que ce qu'elle n'était. En cela, le collectif se réinvente par rapport au dispositif technique et à son vaste appareillage de contrôle. À tous ces égards, l'entreprise de cette relation devient celle d'un affrontement dans lequel les entités en mouvement cherchent à complexifier la lutte de son adversaire, à la rendre impossible. Elle fait émerger de surcroît des luttes de pouvoir. Et comme l'indique Foucault : « toute situation de pouvoir vient avec une stratégie de lutte » (1994 : 1060).

Conclusion générale : Technicisation de la visibilité sur internet

Comment s'articule la relation entre un dispositif technique et un groupe extrémiste ? Quelles formes de visibilité cette co-constitution configure-t-elle ? C'est à ces principales questions de recherche que la thèse a souhaité répondre. L'objectif de cette thèse ne se limite donc pas à étudier les effets d'internet sur l'activisme, comme la littérature a tendance à le faire. Il s'agit plutôt d'une analyse qui renouvelle le modèle de la visibilité médiatisée des militants dits extrémistes en tenant compte des reconfigurations mutuelles entre les technologies du web et l'usager activiste. Pour ce faire, nous avons suivi quotidiennement les interactions en ligne des militants de l'État islamique, tout en portant notre attention aux interfaces et aux infrastructures numériques.

En combinant les idées de la théorie de l'acteur-réseau, les travaux de Suchman sur les reconfigurations humain-machine et les *software studies*, cette étude contribue à une meilleure compréhension de la visibilité des groupes extrémistes sur les plateformes numériques. Nous avons argué tout au long de la présentation de nos résultats que cette visibilité est relationnelle, technicisée et conflictuelle. Par ce fait, il ressort de notre étude que la visibilité est un processus non linéaire, qui se façonne au cours d'épreuves répétées. Chacune de ces épreuves marque la possibilité pour les usagers militants et les plateformes numériques de se réinventer dans un nouvel usage ou d'articuler de nouvelles réponses.

En examinant le fonctionnement de la visibilité de l'État islamique sur les plateformes numériques, nous avons détaillé comment l'État islamique organise et comprend les technologies numériques comme un champ de bataille (chapitre 5). Nous avons ensuite enquêté sur la concrétisation d'un ensemble de rationalités opérationnelles et technicisées qui servent à capter l'attention des partisans et des adversaires (chapitre 6). Puis, nous nous sommes intéressés aux anti-programmes qui tâchent de contrecarrer le projet jihadiste au sein du web (chapitre 7). Nous avons finalement décrit comment l'État islamique met en place des actions de résistance à la modération (chapitre 8).

Nos chapitres de résultat nous ont permis de décrire un ensemble de dimensions caractéristiques de la visibilité des groupes qualifiés d'extrémistes. De là, nous avons formulé quatre propositions. Premièrement, la visibilité des groupes radicaux sur internet est une

entreprise complexe. Elle nécessite un vaste réseau d'actants, ainsi qu'une diversité de modes organisationnels à la fois centralisés et décentralisés. Deuxièmement, l'observation des pratiques quotidiennes suggère que le travail de visibilité suit des objectifs d'amplification et d'abondance du flux informationnel. Ces objectifs sont guidés par un ensemble d'opérations tactiques et automatisées qui requiert l'association et la stabilisation des militants de l'État islamique et de matières informatiques. Troisièmement, il existe une série de contraintes et de forces ennemies qui contrecarrent le projet de visibilité de l'État islamique. Dues aux nombreuses pressions gouvernementales et législatives, les plateformes numériques ont été obligées de favoriser le développement d'un environnement hostile et contraignant à l'égard des contenus jugés extrémistes. Le quotidien de la visibilité du collectif est ainsi devenu celui de la modération et de l'exclusion. Quatrièmement, nous avons suggéré que les partisans de l'État islamique se transforment en habiles bricoleurs et tacticiens afin de limiter les effets négatifs de la modération. Ce constat invite à considérer la modération en tant qu'objet de lutte et d'évitement.

Dans la première section de ce chapitre, nous résumerons l'argumentaire développé jusqu'à présent. Plutôt que de suivre l'ordre des chapitres précédents, nous articulerons nos résultats autour de trois concepts essentiels de notre cadre théorique : l'assemblage, l'action et la reconfiguration. Dans un deuxièmement temps, de manière à rendre notre argument plus général et cohérent, nous introduirons et détaillerons notre proposition, celle d'une *visibilité technicisée*. Dans la troisième section, nous résumerons nos principales contributions. Enfin, nous terminerons en exposant des pistes pour des recherches futures.

Configuration de la relation entre le dispositif technique et les protagonistes de l'État islamique

Être visible pour les protagonistes de l'État islamique s'inscrit dans le programme d'action plus général d'une guerre médiatique. Tel que nos données le révèlent, l'État islamique a – par un enchaînement de ritualisations, de tactiques et de procédés discursifs – apprivoisé internet comme un espace militarisé. Dans les discours des militants, internet est communément appréhendé comme une arme ; comme un front de bataille. Les stratégies et les métaphores belliqueuses abondent. Cela nous permet d'insister sur le fait qu'internet n'est pas un dispositif technique unique, stable et universel. Les contextes d'internet sont bien plus variés que ne le laisse entendre le tropisme cyber-utopiste. Ces discours utopistes

essentialisent une figure très homogène d'internet, en survalorisant ses effets émancipateurs et démocratiques. Or, notre étude de cas est une illustration exemplaire de la « flexibilité interprétative » (Bijker et al., 1987) de la technologie. L'État islamique « décode » (Hall, 1994) les technologies du web selon un mode différent que ce que ses concepteurs ont imaginé. Rappelons-le, pour les concepteurs des plateformes numériques, internet doit être « une force au service du bien » (Twitter, 2019). L'État islamique a radicalement bouleversé cet utopisme, en donnant aux plateformes numériques un nouveau rôle symbolique et social : celui d'agent du contrôle social.

Il n'est toutefois pas question de tirer la conclusion hâtive que la technologie serait « neutre » et qu'elle serait pervertie par de « mauvais » usages. Dans le cadre de notre thèse, nous nous sommes davantage appuyés sur des travaux qui privilégient une approche symétrique entre les usagers et les concepteurs des dispositifs techniques (Akrich 1992, 1995, 2006 ; Suchman, 2007). Certes, les concepteurs des machines configurent l'usager (Woolgar, 1991), mais ces derniers ont également une autonomie dans l'appropriation et la domestication du dispositif technique (Silverstone, 1994). Cette question de la reconfiguration entre le dispositif technique et l'usager a traversé l'ensemble de notre travail. Dans le cas de l'État islamique, on a assisté à une gradation continue de ce processus de reconfiguration entre les plateformes numériques et les militants de l'État islamique. Celle-ci naît d'un réalignement constant du réseau technico-jihadiste qui se défait et se transforme inlassablement face à un partenariat avec les technologies du web on ne peut plus conflictuel. En questionnant ces reconfigurations, il importe de retracer l'articulation du réseau technico-jihadiste et les actions menées en son sein.

Assemblage

Tel que suggéré dans notre cadre théorique au chapitre 3, nous avons réalisé à travers notre étude de cas que la visibilité articule un réseau hybride d'entités humaines et non-humaines. Les éléments qui constituent la visibilité en ligne de l'État islamique font nombre ; elle est le fruit d'interactions entre du code, des corps, des infrastructures, des plateformes numériques, des algorithmes, des professionnels, des amateurs, des matériaux médiatiques, des agents automatisés, des inscriptions et des langages. Ainsi, parler de visibilité en ligne c'est parler de multiplicité. C'est la situer dans ses couches techniques, comme la littérature nous l'a

enseigné (Badouard, 2014 ; Cardon, 2009 ; Lessig, 2006), et humaines. La diversité des actants qui composent la visibilité nous permet d'insister sur trois points.

1° On assiste conjointement à une complexification du tableau de la visibilité. En tenant compte de l'ensemble de ces entités, de leur souplesse et de leur normativité, nous avons montré que la visibilité du collectif juxtapose des dynamiques à la fois horizontales et verticales, globales et locales, centralisées et décentralisées. Cela a pour conséquence de fabriquer une série d'alignements qui sont, à certains égards, extrêmement opaques. Cette superposition de modèles organisationnels démontre que l'utilisation des plateformes numériques par les militants combine plusieurs technologies et pratiques (Dahlberg-Grunberg, 2016 ; Tufekci et Wilson, 2012 ; Treré, 2012, 2018 ; Treré et Mattoni, 2016). Comme nous l'avons indiqué dans le chapitre 5, internet n'est finalement que la suite d'une longue chaîne de médiation qui permet à l'action de visibilité de se produire.

2° Ces liens se tissent dans un contexte particulier : celle d'une logique de la production d'un flux informationnel. Notre enquête a rendu compte d'un aspect fondamental de la visibilité : la visibilité ne forme pas qu'un « voir » ou pour reprendre la terminologie d'Arendt (1961) elle ne concerne pas seulement l'œuvre. Elle reste en même temps un travail de production avec des étapes aussi concrètes que la création et la sélection d'énoncés et de leur distribution, comme les chapitres 5 et 6 l'illustrent. C'est face à cette large palette d'actions que nous avons constaté que la visibilité du collectif travaille activement à former des coopérations entre une série de corps disciplinés et de techniques. Nous avons par exemple décrit dans le chapitre 5 la manière dont le collectif cherche à élargir ses coopérations à un réseau d'acteurs plus décentralisés. Par ailleurs, notre enquête montre que la capacité d'agir n'est pas seulement l'apanage des humains. Les agents automatisés sont pleinement intégrés dans le fonctionnement de la propagande de l'État islamique. Toutefois, toutes les entités n'ont pas le même désir ou la même imposition dans le travail productif de la visibilité, comme les plateformes numériques qui cherchent à se défaire de leur rôle d'hébergeur de contenu (voir chapitre 7). Ces points de fractures et de conflits démontrent que le réseau hybride sous-jacent à la visibilité de l'État islamique est à la fois incertain et vulnérable.

3° Mais l'effet potentiellement le plus important de ces assemblages est que, malgré ces points de rupture, ils dotent le collectif d'un pouvoir habilitant. Autrement dit, en tant qu'ils forment la capacité d'agir du collectif dans le travail de production, de distribution et de

contournement des sanctions. On a par exemple particulièrement évoqué la fétichisation de l'efficacité qui traverse le collectif. Nous avons vu dans les chapitres 5 et 6 que le collectif s'efforce de professionnaliser sa visibilité et de la distribuer le plus largement possible au sein des plateformes numériques. Simultanément, il brave les entraves qui le dévient de son objectif, comme le montrent les chapitres 7 et 8. En cherchant à assurer sa visibilité, ainsi que sa durabilité, l'action se déploie à travers un « pouvoir de la délégation » entre des compétences machiniques, techniques et humaines. Chacune des tâches de fabrication, de distribution et de résistance dépend d'un agencement humain et non-humain singulier. Par exemple, les agencements qui permettent de créer de fausses amplifications ne seront pas les mêmes que ceux qui fabriquent des énoncés ou encore des comptes de réseaux sociaux réservistes. Chacun des agencements mobilise son propre registre de partage de compétences. Celui-ci peut aller de la tâche de création et de l'orchestration, à celle de distribution mécanisée en passant par la stratégie. C'est ce que la prochaine section explore plus en détail.

Séquentialité de l'action

Étonnamment, la littérature sur la mobilisation en ligne s'est peu intéressée à la question de savoir comment les groupes militants utilisent les technologies du web au quotidien. Elle préfère généralement rendre compte de l'ampleur du rôle d'internet dans l'activisme. En suivant quotidiennement les interactions en ligne de l'État islamique, notre étude complexifie le spectre de l'instrumentalisme. Plus qu'un simple outil, nous pouvons dire qu'internet est une « technologie du quotidien » qui structure une pluralité de « régimes d'action » (Boltanski et Thévenot, 1991). Notre étude fait ressortir que les militants de l'État islamique passent continuellement d'une situation à l'autre. Ils doivent par exemple formuler un cadre d'usage de la technologie ; fabriquer et distribuer des énoncés ; assurer leur cybersécurité ; créer sans cesse de nouveaux comptes et profils de réseaux sociaux ; résoudre ou envenimer des conflits et des disputes. Être visible en ligne nécessite ainsi de s'investir dans une série d'actions et de préoccupations diverses qui sont singulières à internet. Nous rassemblerons dans ce qui suit l'ensemble de ces régimes d'action autour de quatre grands axes, que nous envisagerons sous l'angle d'un travail.

1° *Travailler à un cadre d'usage de la technologie*. Nous avons mis de l'avant dans le chapitre 5 que l'État islamique effectue de nombreuses mises en scène des plateformes numériques et de ses usages à travers des visuels, des vidéos ou encore des textes. La

configuration du dispositif technique par les usagers est conditionnelle à ce que Flichy (2008b) nomme le « cadre d'usage »[127], en référence à la perspective goffmanienne des « cadres de référence ». C'est en quelque sorte la « clé de voûte » de tout un système symbolique et fantasmé, qui instaure un rapport à l'objet technique. En cela, nous pouvons dire que faire exister une reconfiguration, requiert qu'elle soit prise dans un champ symbolique et un imaginaire technologique[128]. Ainsi, le collectif ne se contente pas d'utiliser internet, il le définit et fabrique une série d'histoires et d'images à son propos. Il produit une contre-tendance à l'idéal technocratique des plateformes numériques. Il fonctionnalise et instrumentalise internet dans un combat qui prend corps dans un récit de guerre médiatique long de plusieurs décennies.

On dit qu'internet est une ligne de front ; un espace à envahir. On ne parle pas d'utilisateur, mais de « soldats des médias ». Il est mis en scène dans des configurations qui valorisent sa vaillance, sa force et son professionnalisme. En même temps, cette narration singularise l'usager. Dans ce scénario, il devient la matrice de ce que nous pourrions nommer une « individualisation fonctionnaliste ». En effet, nous avons vu que le collectif postule en théorie que chaque individu est apte, de par son engagement à la cause, à participer à la guerre médiatique et à répondre à l'objectif d'efficacité d'invasion. En cela, la visibilité du collectif a besoin de corps fonctionnels qui propagent leur message au sein d'internet. Ce pouvoir individualisant participe grandement à susciter la collaboration d'un maximum de personnes. Il est intéressant de noter que cette conception résonne avec l'idéologie du web social et son architecture qui valorise l'autonomie des internautes en matière de publication (Beer et Burrows, 2007 ; Benkler, 2009 ; Proulx, 2011 ; Proulx et al., 2011).

Avisons pour terminer que cette reconfiguration des technologies numériques en tant que ligne de front n'est pas le seul fait de l'imaginaire et du discours. Des auteurs tels que Suchman (2007, 2012) et Barad (2007) rappellent à juste titre que la configuration humain-machine tient sa forme dans du discursif, mais aussi du matériel. Nous détaillerons dans la section qui suit l'ensemble des logiciels et du matériel informatique, ainsi que les innombrables pratiques qui participent à reconfigurer les technologies numériques.

---

[127] L'auteur définit le cadre d'usage comme « celui qui décrit le type d'activités sociales proposées par la technique, qui la positionne dans l'éventail des pratiques sociales, des routines de la vie quotidienne, et précise les publics envisagés, les lieux et les situations où cette technologie peut se déployer » (Flichy, 2008b :164).

[128] Notons qu'il ne s'agit pas ici d'envisager la performativité dans le seul ordre du discours. Suivant l'approche de Boltanski et Thévenot (1991), chacun des régimes d'action fonctionne l'un à côté de l'autre.

2° *Travailler à la production et à la distribution du flux informationnel*. Nous avons montré dans le chapitre 5 et le chapitre 6 que le collectif produit activement des énoncés. Ces derniers peuvent être produits de façon centralisée et décentralisée. Que ces énoncés soient officiels ou non, ils correspondent à la première étape de production de l'information ; celle qui consiste aux opérations de réduction et de sélection. En cela, le monde de l'État islamique se transpose dans des formats accessibles à une large audience. Il se simplifie et se réduit dans un ensemble de photographies, de vidéo, d'enregistrements sonores, de textes et de mèmes. Nous avons décrit plus amplement dans le chapitre 6 le second mouvement qui fait suite à cette première étape de production ; celui qui transporte et véhicule ces matériaux médiatiques. Nous avons alors constamment utilisé le concept d'*abondance* pour désigner le programme d'action d'amplification dans lequel s'inscrit la distribution du matériel médiatique.

Pour ce faire, le collectif a tiré parti de la strate computationnelle pour mécaniser et manipuler l'amplification de ses contenus. Ces opérations résultent d'un travail habile de manipulation de la matière informatique qui, comme nous l'indique MacKenzie (2003a), se resserre dans des circuits toujours plus interconnectés. Ces non-humains composés de code sont ici mobilisés dans diverses configurations. Premièrement, le militant opère une série de manœuvres à travers l'exploitation de plusieurs *affordances* offertes par les plateformes qui lui permettent d'accentuer sa visibilité. Dans le chapitre 6, nous avons illustré comment les protocoles, les algorithmes et les fonctionnalités programmatiques de Twitter ont généré d'innombrables possibilités en matière de visibilité et d'abondance. Ces non-humains sont donc un constituant actif dans les pratiques de visibilités. Mais pas seulement, ces derniers traduisent également une forme plus technicisée et abondante des stratégies de présentation de soi. En développant une série de fonctionnalités qui facilitent le partage, l'interaction et la sociabilité, les plateformes numériques technicisent une série de pratiques qui rendent possibles la viralité et la popularité. Au terme de cela, nous pouvons dire que les militants n'interagissent pas seulement avec des utilisateurs ; mais avec des algorithmes et du code qui oriente leur visibilité selon des paramètres prédéfinis. Ils sont les nouveaux médiateurs qui forment les routines quotidiennes de visibilité des internautes.

Par ailleurs, nous avons insisté sur l'importance que jouent les agents automatisés dans les interactions quotidiennes du collectif. L'habileté du collectif est donc aussi celle de la programmation d'automates qui sont de plus en plus normalisés au sein des plateformes numériques. Par exemple, le chapitre 5 indique que sur Telegram, les *botnets* occupent

plusieurs rôles. Ils peuvent propager de la propagande ou encore assurer la régulation des chaînes. Dans le chapitre 6, nous avons vu comment les *botnets* sont mobilisés sur Twitter dans des actions plus stratégiques de manipulation de l'attention. Les militants les ont notamment utilisés pour fabriquer de fausses amplifications. Cela nous a permis d'illustrer que ces agglomérats de code sur Twitter sont dans le cas de l'État islamique peu sophistiqués et s'apparentent plutôt à des comptes de *spammer*. Mais, de toute évidence, que ce soit sur Telegram ou sur Twitter ces agents automatisés ne cherchaient pas à imiter le comportement humain. Ils étaient là pour délivrer une performance spécifique ; celle d'augmenter la vitesse de propagation des flux informationnels. En propageant leur contenu par le biais d'agents automatisés, le collectif consolide l'image d'une politique qui se veut toujours plus technicisée et abondante.

Nous avons conclu dans le chapitre 6 que ces agents automatisés n'avaient pas pour vocation de remplacer l'humain dans la tâche de distribution. Ces derniers doivent être pensés à côté d'eux. Les militants restent d'actifs contributeurs dans la distribution de contenus et combinent divers usages. Ils peuvent être autonomes en créant et partageant leur propre contenu. Ils peuvent aussi adopter des formes automatisées en propageant machinalement les énoncés officiels ou non officiels par le bouton du *retweet*, partage ou *like*. En ces termes et dans les configurations les plus extrêmes, l'usage est porteur de certaines figures de l'automate.

L'un des aspects importants qui ressortent de notre analyse est que ces programmes d'abondance généralisent des comportements qui nuisent à la conversation publique. Nous l'avons vu, les partisans galvanisent l'attention en tirant parti de la matière informatique et des *affordances* numériques. Ils cherchent à faire du bruit. Cela se marque par des comportements qui s'associent rapidement au *spam*, au harcèlement, à la duperie ou encore au *trolling* (voir chapitre 6 et 7). Les partisans n'obéissant plus aux règlements des plateformes numériques, ils s'organisent par des mécanismes de viralité qui dépassent les normes prévues par celles-ci. Ils usent de ces services pour des actions agressives et trompeuses.

3° *Travailler à faire d'internet un espace antagoniste*. Si la réalité en ligne de l'État islamique se bâtit sur des opérations conçues pour mener une guerre médiatique, l'une des résultantes est qu'il stimule à bien des égards des situations d'antagonismes et de disputes. Davantage qu'une sphère publique délibérative, notre étude de cas montre qu'internet est indissociable

de dimensions conflictuelles. En cela, internet contient de multiples ordres et désordres. Il est pluriel et s'oriente vers un champ agonistique. À certains égards, cela se rapproche de la conception de Mouffe (2000, 2005) qui pose le concept de pluralisme agonistique comme alternative à la sphère publique délibérative habermasienne. Pour Mouffe (2010), la politique est inéluctablement plurielle et conflictuelle. Elle instaure de ce fait des distinctions constantes entre *eux* et *nous*. Notre analyse se dégage toutefois de celle de Mouffe sur certains aspects. Dans sa conception, l'opposant est un acteur légitime et n'est pas un ennemi à abattre. Dans notre étude de cas, l'antagonisme entre les adversaires est bien plus virulent. Elle intègre des alliances et des ruses qui ont pour objectif d'annihiler l'ennemi.

En retraçant les différentes démarches à l'œuvre dans ces situations conflictuelles, nous avons montré à travers le chapitre 6 et 7 que l'antagonisme se construit de plus en plus dans et par la matérialité. Cela permet de jeter un nouveau regard en ce qui concerne les configurations conflictuelles entre protagonistes. Par exemple, nous avons vu que les actions pouvaient être menées entièrement par des *botnets* qui s'affrontent dans des luttes iconographiques ou encore qui signalent massivement des comptes d'adversaire. L'interaction se passe alors entre des machines qui s'attaquent réciproquement. De là, notre enquête a soulevé une série d'effets. Ces interactions machines-machines inscrivent les luttes dans de nouvelles configurations d'espace et de temps. Elles promulguent des luttes immédiates, c'est-à-dire qu'elles peuvent être menées simultanément dans différents espaces et à des vitesses qui dépassent les capacités humaines. Ce qui innerve ces conflits, c'est de paralyser momentanément le narratif de l'ennemi en l'excluant de la plateforme ou alors en l'inondant de contenus rivaux. En d'autres mots ; elles font taire ou surexposent l'adversaire à une masse de contenus. En l'occurrence, ces combats matérialisés et le plus souvent anonymes favorisent et amplifient l'antagonisme. Ainsi, l'enrôlement du code informatique est un allié non négligeable dans la tâche du combat. Ce type d'action rappelle que l'une des matières premières des conflits en ligne met en œuvre des machines, du code, de l'énergie et des méthodes. Ces dispositifs de natures automatisés contribuent à façonner un espace dans lequel les effets sont subséquents à des efforts de quantification et d'abondance.

4° *Travailler à réduire les incertitudes*. Un point important qui ressort de notre analyse concerne l'ensemble des situations d'indéterminations qui parcourent la visibilité du collectif. Rappelons que pour l'ANT, la société n'est jamais donnée a priori. En cela, « la société est le résultat toujours provisoire des actions en cours » (Callon, 2006 : 2). Ce principe exprime

l'idée qu'il existe une part d'incertitude et d'imprévisible dans l'action. En d'autres termes, l'action se produit dans des épreuves répétées au cours desquelles le réseau peut se défaire ou se transformer (Licoppe, 2010). Le succès d'une action n'est en cela jamais garanti. Ainsi, l'auteur rappelle que « le risque d'échec de l'action n'est pas d'ordre contingent. Il est structurel et constitutif de toute opération performative » (2010 : 3-4). Cet aspect d'indétermination relative dans l'action ressort particulièrement dans le réseau technico-jihadiste que nous avons étudié. Notre enquête démontre que le collectif doit continuellement se défendre de multiples interférences.

Ces points d'incertitudes le font accéder à une autre dimension de la visibilité ; celle de devoir agir dans un monde toujours plus incertain. En cela, sa visibilité n'est pas inerte, mais est infusée de transformation et de résistance. Si les plateformes numériques créent de nouvelles possibilités, elles fabriquent simultanément de nouvelles contraintes. Nous avons ainsi décrit une série d'anti-programmes qui exposent l'État islamique à de multiples dangers et visent à contrecarrer son projet en ligne. Mentionnons pour commencer qu'en bâtissant sa visibilité sur des plateformes numériques, elles l'exposent à plus de risque de surveillance et de traçabilité de la part des compagnies privées, des gouvernements, de logiciels espions et des *hacker*. Par ailleurs, le risque de surveillance dépasse la simple collecte de données par les entreprises propriétaires des plateformes numériques. Par exemple, nous avons indiqué que certains acteurs malveillants font circuler des fausses versions de leur dernière production médiatique en y intégrant des logiciels espions. Une autre menace dont le collectif doit se prémunir est la propagation de fausses informations à leur égard. Nous avons dit dans le chapitre 5 que le collectif multiplie les appels à vérifier l'information propagée en raison des faux communiqués qui peuvent circuler. Indiquons ensuite l'écosystème de la modération qui a plongé le collectif dans une incertitude permanente quant à la performance de son action. Le profil, le groupe ou la chaîne d'un militant peuvent à tout moment être supprimés de la plateforme numérique. L'action ne se forge plus dans un temps programmé et infini, mais dans celui de l'imprévu et du limité. Le temps de la visibilité est ainsi lié à l'autorité des plateformes numériques.

En adoptant des perspectives telles que celles de l'ANT et de Michel de Certeau, nous avons toutefois vu que les anti-programmes reconfigurent le réseau autour de nouveaux programmes d'action. Par conséquent, le collectif se réactualise continuellement dans de nouvelles identités et de nouvelles tactiques. Dans le chapitre 5, nous avons illustré les spécialistes en

cybersécurité qui travaillent quotidiennement à assurer la sécurité opérationnelle du collectif en produisant de nombreux contenus, PDF et communiqués. Face au risque accru de traçabilité, il n'a donc d'autres solutions que d'instruire les autres militants aux risques et aux précautions à prendre. Le choix des mesures se traduit dans des mesures d'auto-défense qui incitent les militants à faire un usage abondant de techniques de chiffrages et de cryptages ainsi que des sites d'anonymisation tels que par exemple le réseau TOR.

Au chapitre 8, nous avons analysé comment le collectif essaye de résister à la modération. Nous avons suggéré que le collectif introduit un nouveau programme d'action : celui de la désobéissance et de l'anti-discipline. Cela passe par une série de transgressions, de manipulations techniques, de solidarités et de mobilités. Notre enquête contribue ainsi à montrer que les plateformes numériques peinent à « discipliner l'utilisateur » (Thévenot, 1993). Dans notre étude, l'usager se reconfigure dans des usages qui provoquent des ripostes inattendues. Ainsi, si la viabilité des comptes, chaînes et groupes pro État islamique n'est pas infinie, il est frappant de constater en revanche le caractère ininterrompu de leur flux informationnel.

Reconfiguration

Nous avons largement souligné dans notre cadre théorique que les entités humaines et non-humaines se reconfigurent mutuellement et perpétuellement. Les identités ne sont jamais stabilisées, tout comme les frontières entre machine et humain ne sont pas données a priori. Dans la lignée des travaux de Suchman (2007), notre étude suggère d'envisager cette constitution mutuelle au travers des différentes contraintes qui animent la relation humain-machine. Jusqu'à présent, la littérature a principalement rendu compte de reconfiguration entre des dispositifs techniques et des usagers ordinaires dans des alignements plus ou moins stabilisés et harmonieux. Notre enquête contribue à complexifier les schémas de la reconfiguration en démontrant comment un utilisateur indésirable réajuste et réorganise l'aménagement d'un dispositif technique. Les résultats de notre étude dévoilent que la visibilité du collectif se dissout dans un champ d'assemblage socio-technique complexe et instable. Les potentialités démocratiques des technologies du web qui articulaient naguère les jihadistes au dispositif, ont disparu, ou n'ont laissé que des fragments. En effet, au fil de l'analyse, nous avons découvert que les plateformes numériques devenaient le lieu de tous les affrontements. Bien loin d'un assemblage harmonieux, l'ajustement entre les plateformes

numériques et les utilisateurs jihadistes fait, pour le moins, l'objet de nombreux points de désaccords et de ruptures.

Dans le chapitre 7, nous avons vu qu'à un moment donné les plateformes numériques ont fait l'objet d'une série de controverses en raison de la propagation des discours extrémistes en leur sein. Face aux multiples pressions gouvernementales et à un environnement juridique de plus en plus contraignant, les plateformes numériques ont été contraintes de réaligner leur politique de modération. Pour reprendre la notion de Barad (2007), celles-ci ont opéré de nouvelles « coupures agentielles » qui ont renforcé la frontière entre utilisateurs légitimes et illégitimes. La force d'intervention de ces nouveaux découpages est de créer des impossibilités inédites pour un certain public visé. Dans le cas étudié, nous avons vu que ces derniers sont faits de nouvelles Règles et Politiques, de transformations organisationnelles et d'ajouts de nouveaux artefacts techniques. De manière plus précise, nous avons décrit dans le chapitre 7 comment les plateformes numériques ont renforcé leurs Règles et Politiques, élargi leur équipe de sécurité et matérialisé la tâche de modération dans des dispositifs d'apprentissage automatique. Ces « coupures agentielles » auront des implications politiques, en ce sens qu'elles favorisent de nouvelles rationalités et formes organisationnelles plutôt que d'autres.

Le chapitre 7 de cette thèse a entre autres contribué à dresser le portrait du scénario d'un « solutionnisme technique », au sens où l'entend Morozov (2014). L'idée sous-jacente de ce modèle solutionniste est que les problèmes d'extrémisme peuvent se résoudre par un filtre automatisé. Ainsi, les méthodes d'apprentissage automatique et d'intelligence artificielle ont été propulsées sur le devant de la scène tant par les pouvoirs publics que par les entreprises privées. À cet égard, nos résultats ont illustré la manière dont la modération a été davantage déléguée à un ensemble d'algorithmes, placés sous le pouvoir opaque des plateformes numériques (Burell, 2016 ; Cardon, 2015 ; Pasquale, 2015). Dans cette gradation continue des processus automatisés dans la régulation des flux informationnels, on assiste à une nouvelle industrialisation de la modération. Jusqu'à présent, il n'y a que les grandes plateformes numériques qui disposent des ressources techniques et humaines nécessaires pour appliquer les mesures proactives imposées par de plus en plus de gouvernements. Bien plus, elles disposent des structures de données nécessaires pour entraîner ses algorithmes de détection automatique. Elles s'approprient le pouvoir de voir.

Ces nouveaux régulateurs fabriquent ce que nous avons appelé dans le chapitre 7 des « kits solutionnistes ». Produits selon des standards de l'industrie technologique ces derniers basent leur pouvoir disciplinaire sur base de l'efficacité et de la rapidité d'action, en privilégiant le perfectionnement machinique qui a peu avoir avec les capacités humaines de contrôle. Ces régulateurs centrés sur le flux informationnel concentrent la panoplie de leurs stratégies sur la connaissance, le contrôle et les données. Nous pouvons voir les débuts d'une reconfiguration d'internet vers un ensemble de techniques éditorialistes qui assurent un contrôle a priori du « mauvais » flux informationnel. Le but est que les « mauvais » contenus soient supprimés avant même qu'ils soient visualisés par un internaute. Ces tendances s'écartent des valeurs libertaires promues par les pionniers d'internet, et pointent vers un contrôle plus massif et plus direct à la fois des flux informationnels et des usagers. Entendons-nous, la surveillance ne concerne pas tant l'individu en tant que tel, mais celles d'occurrences probables de contenus et de comportements nuisibles qui doivent être minimisés.

Notre enquête illustre la manière dont cette nouvelle configuration algorithmique fonde une asymétrie nette de la visibilité. Ce « voir automatisé » s'accapare le pouvoir de perception. Il est l'œil technicisé qui agit comme une loupe puissante. Il baigne dans l'opacité et fonctionne sur un monde continu de surveillance et de détection qui coïncide à une norme. Chaque trace est ainsi évaluée et catégorisée. Nous avons mis en relief, lors de notre enquête, que ce voir automatisé ne fonctionne toutefois qu'à partir de catégories construites préalablement par des humains. Les algorithmes suffisamment raffinés et spécifiques pourront ensuite actionner les catégories en analysant le corpus des traces numériques existantes. En d'autres termes, ils rendent visibles et gouvernables les « mauvais » acteurs, contenus ou comportements. Notre étude note que le caractère automatisé de la détection n'exclut toutefois pas les humains. Nous avons montré dans la lignée des travaux de Simondon (1958) que les algorithmes ont besoin de l'humain comme technicien et associé. L'analyse révèle que l'humain reste essentiel pour la conception de l'algorithme et son entraînement et pour discerner le contexte du contenu. Ainsi, comme nous l'avons mentionné dans le chapitre 7, le pouvoir de l'algorithme est distribué entre des humains et des non-humains.

Ici, cette relation fictive avec un dispositif de pouvoir ne fait pas forcément naître un assujettissement des corps, comme dans le modèle du panoptique de Foucault (1975). En fait, notre enquête a démontré que le collectif cherche activement des solutions pour assurer la continuité de son expérience numérique. Nous suivons Dewey (1916, 1929) lorsqu'il affirme

de façon convaincante que les interruptions d'expérience sont des sources d'apprentissage qui ouvrent la voie à une recherche de solutions pour résoudre ces situations. Nous avons ainsi affirmé dans le chapitre 8 que, face à la modération, l'usager jihadiste se reconfigure en tacticien et bricoleur pour assurer la continuité de sa visibilité en ligne.

Militantisme et configuration d'une visibilité technicisée

Jusqu'à présent, ces assemblages complexes nous ont alertés quant aux effets politiques, les frontières changeantes et les reconfigurations possibles entre les plateformes numériques et les militants. Il est maintenant temps de rendre compte des régimes de visibilité que ces agencements particuliers configurent. Cette section nous fait donc plonger au cœur de la thèse. La proposition que nous souhaitons défendre ici est que *dans le contexte contemporain des technologies numériques, la visibilité des militants est de plus en plus technicisée. Elle se fonde sur l'incessant déploiement d'une raison technique, qui généralise un ensemble de comportements nuisibles et de procédures trompeuses, et qui à terme contraindrait le jeu démocratique*. Voyons plus en détail cette proposition.

Visibilité technicisée et raison technique

La thèse a montré que l'apparence publique des militants est produite dans un ensemble de choses et de relations, de plus en plus techniques. En revanche, cette machination optique qui vise à forcer le regard de l'autre sur une cause n'est pas le simple fait d'une accumulation d'artefacts techniques. C'est une activité spécialisée qui exploite la dimension technique et automatisée des technologies numériques avec ses normativités propres. La visibilité devient dominée par les catégories d'un voir technicisé, aussi bien que par une rationalité technique. Nous avons maintes fois argué que la tendance à faire-voir s'articule autour d'un fétichisme de l'efficacité qui trouve sa forme dans et à travers la matière informatique. De cela, la visibilité en ligne n'évince pas les rapports de productivité et de production qui héberge en eux des formes organisationnelles décentralisées et centralisées incarnées par des humains et des non-humains (voir chapitre 5 et 6).

Mais, fabriquer, organiser et distribuer des énoncés ne se fait jamais avec des techniques neutres. On constate que quand les technologies numériques deviennent la forme d'apparence publique par excellence, elles circonscrivent une culture particulière, elles projettent un

monde. Comme nous l'avons vu, le pouvoir de la visibilité est aujourd'hui de plus en plus structuré par des entreprises privées qui ont leur propre univers de discours et d'actions. Elles ont leur jeu à elles, celui d'une combinaison complexe de techniques d'individualisation et d'approches machiniques. Elles démontrent qu'il est « techniquement » possible d'être autonome et de déterminer sa propre visibilité. Elles travaillent sur l'idée que chaque individu est doté d'un pouvoir d'autodétermination sans précédent. Par ailleurs, la rationalité des plateformes numériques ne remet pas en cause le fétiche de l'efficacité, elle le défend plutôt en concentrant le pouvoir d'amplification et d'abondance au sein de fonctionnalités informatiques (comme le *like*, le *retweet*, le partage, les tendances, les *hashtags*) et en normalisant la présence d'agents automatisés en leur sein. Dans ce contexte, les codes techniques qui façonnent la visibilité reflètent des intérêts sociaux et économiques particuliers, ceux d'une accentuation et d'une abondance de contenus qui engagent toujours plus les usagers sur les plateformes.

Des formes de visibilités truquées et délétères

Dans cette quête d'efficacité et d'abondance, les procédures sont souvent suspectes. Dans le chapitre 6, nous avons insisté sur ce point, en montrant comment l'État islamique mobilise et manipule les failles de l'écosystème numériques pour affirmer l'incessante amplification des flux informationnels. Le but d'une telle démarche est de truquer le jeu de la visibilité en amplifiant délibérément l'abondance des énoncés. Certaines tactiques favorisent la duperie en fabriquant de faux comptes pour créer l'illusion d'un consensus. D'autres détournent des *hashtags* et cherchent à accéder aux tendances. Le faire-voir passe aussi par des tactiques qui préconisent le *trolling* et le harcèlement d'autres utilisateurs et sources médiatiques. Par ailleurs, la conception dialogique correspondante relève moins de l'élaboration de longs argumentaires que de la production de nuisances dans la conversation publique. La décentralisation réinvente la distribution de la propagande, qui se traduit dans les mécanismes mêmes des grandes plateformes numériques. Elle se base sur la disposition à l'amplification et à la viralité offertes par les plateformes numériques. Ce type de visibilité technisée met en lumière le risque que la forme dominante du discours politique fonctionne de plus en plus à partir d'un jeu délibéré de duperie et de *trolling*.

Nous avons indiqué que ces comptes et profils sont gérés par des humains, des robots ou par les deux. Toutes les plateformes ne signalent pas nécessairement que le compte est géré par

un *botnet*. Du même coup, le propagandiste devient un être obscur. Il crée de l'indétermination sur son statut machinique ou humain. Cette difficulté à pouvoir discerner l'utilisateur ne découle pas du simple fait que les *botnets* sont davantage sophistiqués. D'ailleurs, nous avons soulevé dans plusieurs cas que les *botnets* restaient à leur statut de pure machine, sans aucune personnification (voir chapitre 6). Mais, comme nous l'avons indiqué dans le chapitre 5, le militant peut se réaliser en tant qu'automate, en perpétuant les rouages d'une automatisation. Ce faisant, l'identité machine-humain se complexifie en attestant simultanément une humanisation du robot et une robotisation de l'humain. Cette manifestation marque le franchissement de la frontière entre l'artificiel et l'organique. Pour reprendre les propos d'Haraway (1991) « la culture technologique de pointe défie ces dualismes de manière insolite. Dans la relation entre l'humain et la machine, il n'est pas aisé de dire qui fabrique et qui est fabriqué » (p.117).

Cette subversion de la frontière ne se contente pas de modifier la forme de l'expression, elle élargit et renouvelle de nouveaux sujets politiques. Ceux-ci se spécifient par une délégation supplémentaire entre les humains et les machines. En d'autres termes, ils se fondent sur une épistémologie du code informatique qui opère des déplacements quotidiens entre des identités organiques et machiniques. Cette hybridation du sujet politique se fait au bénéfice de l'interactivité, de la connectivité et du surpassement de l'espace et du temps exclusifs aux technologies numériques. Notre enquête montre que la politique ne peut plus se penser en dehors d'associations complexes qui allient code, algorithmes, militants, agents automatisés, mécanisations et méthodes.

Rendre invisible l'opposition

Notre enquête révèle une part des limites de cette raison technique et sa force sinistre. De ce mode d'optimisation du visible à des fins de propagande, il ressort de nouvelles relations de pouvoir. Ce modèle d'amplification a ceci de particulier qu'il cherche à exercer un pouvoir sur ses adversaires en les réduisant au silence. Dans cette lignée, la thèse a démontré comment le collectif organise et coordonne des actions qui visent à absorber l'opposition. Nous avons vu que cela peut se faire en submergeant la parole de l'ennemi (chapitre 6) ou alors en l'excluant de la plateforme par des signalements massifs (chapitre 7). L'objectif est ainsi d'agir sur l'adversaire en mettant en échec sa visibilité. Dans ce contexte, le triomphe de la visibilité renvoie à la prise en compte de relations stratégiques et d'affrontements. Nous

pouvons donc dire que la visibilité technicisée n'est pas seulement une accumulation d'artefacts techniques, elle est le fait de relations de pouvoir, médiatisées par des techniques. Au chapitre 6, nous avons indiqué que ces tactiques induisent le risque de porter préjudice à l'exploration du Multiple. Ce constat fait écho aux travaux de Marcuse (1968) à propos de ce qu'il nomme la « pensée unidimensionnelle ». Il décrit celle-ci comme mettant en échec la logique de la contradiction. Elle porte en elle la tyrannie du discours clos et homogène. D'une certaine manière, elle contredit la condition politique essentielle de la pluralité (Arendt, 1961, 1995) et mène à des espaces de plus en plus polarisés.

En même temps, la visibilité technicisée se bâtit sur un système inéquitable. Tout au long de notre enquête, nous avons montré que le rôle de l'expertise technique est devenu une compétence primordiale dans l'administration de la visibilité. Celui qui domine son adversaire est celui qui manœuvre au mieux les ressources techniques des plateformes numériques et qui garde une longueur d'avance sur la modération. Curieusement, les vertus de la décentralisation tant ventée par les cyber-utopistes n'ont pas mené aux effets de démocratisation tant espérés. Il n'est pas question ici de nier l'effet émancipateur que peut avoir internet. Plutôt, il s'agit de reconnaître que les formes décentralisées de participation peuvent aussi être porteuses de nouvelles asymétries et de nouveaux principes de domination et nuire au bon déroulement du débat en ligne. Finalement, ce qui réside dans ces mécanismes c'est la transformation du jeu même de la démocratie ; celle-ci devant composer avec un univers technologique de plus en plus polarisé et truqué.

Contributions de la thèse

En portant notre analyse sur ce qui sous-tend la visibilité en ligne de groupes qualifiés d'extrémistes, et sur ce qui la trouble, notre thèse apporte plusieurs contributions à la littérature scientifique. Ces contributions s'inscrivent dans le cadre des débats relatifs au militantisme en ligne, à la visibilité des mouvements sociaux et à l'usage d'internet par des groupes radicaux.

D'un point de vue spécifique, notre recherche documente le cas inédit de l'État islamique. Alors que la littérature a eu tendance à porter son attention sur la sophistication de la propagande de l'État islamique (Mahlouly et Winter, 2018 ; Lorenzo-Dus et Macdonald, 2018 ; Saltman et Winter, 2014 ; Winter, 2015, 2018 ; Zelin, 2015), nous disposions de peu de

connaissances sur la dynamique de sa visibilité en ligne. De plus, concernant le jihadisme en ligne, les études sur le terrorisme, notamment en criminologie, tendent à privilégier les questions relatives à la radicalisation sur internet et à la manière dont internet est utilisé pour atteindre des objectifs stratégiques (Awan, 2007b ; Bockstette, 2009 ; Conway, 2012, 2014 ; Gill et al., 2015 ; Huey, 2015 ; Rudner, 2017 ; Pearson, 2016). Ce faisant, rares sont les études qui se sont intéressées à l'usage quotidien de cette technologie par des groupes extrémistes.

En se détournant des questions de radicalisation et des usages utilitaristes d'internet, notre thèse adopte une perspective renouvelée des enjeux relatifs à l'extrémisme en ligne. Effectivement, notre étude se détourne du réductionnisme technique et met en perspective la nature dynamique de la visibilité en ligne de groupes radicaux, en faisait ressortir qu'elle est relationnelle, technicisée et conflictuelle. Notre recherche montre la diversité des acteurs (militants, agents automatisés, matérialité informatique) investis dans la diffusion de la propagande, les dispositifs mis en place pour la réguler (lois et règlements, modération, cyber-vigilantisme) et la cyber-résilience des militants.

À ce titre, notre thèse insiste sur le fait que la visibilité en ligne est cacophonique, brisée et cahotante. L'action collective dépend d'acteurs et de technologies, multiples et épars ; tout en étant intimement liée à de nombreux échecs et détournements en raison d'intenses leviers régulateurs mobilisés pour contrôler les flux informationnels indésirables. Nous avons souligné que ces assemblages complexes participent à structurer ces technologies du quotidien à partir de plusieurs régimes d'actions. Quatre formes d'actions peuvent résumer la dynamique de la visibilité en ligne : cadrer l'usage des technologies ; produire et distribuer le flux informationnel ; faire de l'objet technique un espace propice aux antagonismes ; réduire les incertitudes.

Ainsi, notre thèse montre comment ces luttes pour la visibilité font intervenir de nouveaux acteurs, de nouvelles pratiques et de nouvelles méthodes. Certains de ces aspects ont déjà été étudiés de façons séparées dans la littérature, mais peu d'études ont cherché à penser leur interrelation. Pareillement, rares sont les travaux qui ont considéré sérieusement le rôle de la matérialité informatique dans les processus de visibilité et d'invisibilité de groupes jihadistes. En pensant l'hétérogénéité de la visibilité, notre recherche offre un éclairage plus subtil et nuancé du fonctionnement de la visibilité en ligne.

Par ailleurs, notre étude montre que les stratégies de communication de l'État islamique poursuivent des objectifs largement documentés au sein de la littérature sur le terrorisme : mise en scène de la violence, usage prépondérant de l'iconographie et de l'audiovisuel, distribution des actualités jihadistes, de communiqués, de directives opérationnelles, de formations. Cependant, ces stratégies font intervenir, à l'ère des plateformes numériques, de nouveaux acteurs, de nouveaux formats, de nouvelles rationalités et de nouveaux contrôles informationnels. Les technologies numériques renouvellent ainsi les luttes d'informations d'une autre manière. L'automatisation se normalise de manière à amplifier les messages et créer une économie de l'abondance ; les formats visuels sont largement privilégiés ; la distribution fait intervenir des formes centralisées et décentralisées ; les messages sont distribués à une audience diversifiée ; les mesures de surveillance, de censure et de contrôle de l'information sont en grande partie opérées par les intermédiaires techniques.

La manipulation de l'attention a suscité un intérêt particulièrement fort au sein de l'extrême droite et d'autres sous-cultures présentent sur internet (Benkler et al., 2018 ; boyd, 2017 ; Marwick et Lewis, 2017 ; Phillips, 2015, 2018) et, dans une moindre mesure, dans la littérature sur le jihadisme. En montrant comment l'État islamique manipule l'attention, nous avons documenté ces évolutions récentes de manière à les rendre plus faciles à appréhender.

D'un point de vue plus global, la présente recherche contribue à une meilleure compréhension de la visibilité en ligne des groupes qualifiés d'extrémistes. À ce titre, plusieurs enseignements plus généraux peuvent être tirés de notre étude de cas. Ceux-ci se déploient principalement sous trois dimensions. Premièrement, en ce qui concerne les études sur les mobilisations en ligne, notre recherche contribue à un nouvel éclairage de l'activisme contemporain par l'attention particulière qu'elle accorde aux logiciels et à la matérialité informatique. Notre thèse fournit un exemple de façon d'aborder de manière critique la visibilité en ligne de groupes activistes, en interrogeant les conditions matérielles dans lesquelles elle se déploie. En partant de la théorie de l'acteur-réseau, de la reconfiguration de Suchman et des *software studies*, nous avons montré l'intérêt de prendre en compte l'usager activiste et les logiciels, ainsi que la manière dont ils se co-constituent. L'interrelation complexe entre les militants et la matérialité informatique a pour sa part souvent été ignorée, voire absente des études sur les mouvements sociaux.

Cette thèse donne ainsi une image de l'activisme en ligne qui dépasse le spectre de l'instrumentalisme et du fonctionnalisme. Notre contribution à l'étude de l'activisme en ligne est d'avoir offert une analyse détaillée qui prend en compte les schémas d'action sur le web des militants. Cela nous a permis de considérer davantage de dimensions en ce qui concerne l'activisme en ligne. Nous avons montré que les militants interagissaient avec un ensemble d'interfaces, de plateformes, de fonctionnalités informatiques, de matériels médiatiques et d'agents automatisé pour faire fonctionner leur visibilité. Nous avons argué que pour être visible en ligne, l'action mélange une série d'actions qui se trouvent à la fois en dehors et sur les plateformes numériques. Par ailleurs, nous avons mis l'accent sur la manière dont ces entités en relation se configuraient et reconfiguraient à travers des opérations de cadrage, des tactiques, des coopérations et des trahisons.

L'idée même de rétablir une complexité dans l'écosystème médiatique des activistes a déjà été soulevée par plusieurs auteurs. Ces études ont soutenu l'importance de considérer l'ensemble des technologies de communication utilisées par les activistes (Dahlberg-Grunberg, 2016 ; Treré, 2012 ; Treré et Mattoni, 2016 ; Tufecki et Wilson, 2012). D'autres travaux ont montré la complexité de l'activisme en ligne en rendant compte des configurations en ligne et hors ligne (Castells, 2007 ; Gerbaudo, 2012 ; Sassen, 2002 ; Jurgenson, 2012), articulant une *choregraphy of assembly* (Gerbaudo, 2012). Jusqu'ici, la complexité communicationnelle des mouvements sociaux a donc été abordée de deux manières. Pour les uns, il s'agit de dépasser le parti pris d'un média unique, et pour les autres de dépasser le dualisme numérique. Si notre étude prolonge cette réflexion, elle en élargit aussi la gamme, en montrant la diversité des acteurs humains et non-humains qui interviennent dans la visibilité. Accentuer la complexité de l'action en ligne permet de dépasser le vocabulaire dualiste largement répandu au sein de la sociologie des mouvements sociaux, un vocabulaire qui tend à perpétuer la dichotomie humain/non-humain, technique/sociale.

Deuxièmement, nous avons développé le concept de visibilité technicisée. Avec cette notion, nous entendons reconnaître deux faits simultanés : les réseaux techniques sont de plus en plus déployés dans la constitution de la visibilité ; qui marque l'extension d'une raison technique, non pas en tant que domination de la technique, mais d'un fétichisme de l'efficacité qui trouve sa forme à travers la matérialité. Nous avons largement insisté sur le fait que cette

expansion des réseaux techniques n'est pas réductible à un « tout technique », mais s'organise dans un réseau hybride d'entités humaines, d'entités non-humaines et de formes discursives.

Notre proposition s'affranchit d'une épistémologie déterministe qui tend à comprendre les médias de communication comme une simple extension de la perception sensorielle humaine et de la communication dans l'espace et dans le temps. Au lieu de cela, elle permet une approche plus dynamique de la visibilité en redistribuant l'action parmi plus d'agents que ne le prévoit le scénario déterministe. Dans la visibilité technicisée, la visibilité est le fruit d'une longue chaîne de médiation d'entités humaines et non-humaines qui cherchent à se stabiliser. De plus, l'ancrage relationnel de la visibilité que nous proposons dépasse la relation humaine entre celui qui voit et celui qui est vu, comme cela a traditionnellement été le cas dans les études sur la visibilité (Brighenti, 2010 ; Simmel, 1908 ; Thompson, 2005 ; Voirol, 2005b). Partant de l'ANT, la notion de visibilité technicisée permet de rendre compte du rôle actif des non-humains dans la construction et la fabrication de la visibilité.

Si la visibilité technicisée confère du pouvoir aux utilisateurs pour assurer leur visibilité, nous avons en même temps émis certaines réserves quant à la valeur réelle de ce faire-voir. Notre thèse remet en cause le modèle idéaliste qui conçoit la vision comme un accès privilégié à la connaissance du monde. Nous avons montré qu'en s'intéressant à la manière dont se constitue la visibilité, on s'aperçoit qu'à certains moments cela nécessite des trucages et des duperies. En cela, celle-ci peut devenir une vaste entreprise de duperie qui piège l'Autre dans l'illusion. Elle assure un voir biaisé et parfois violent, qui découle de rapports de domination et d'asymétrie. Par ce fait, elle n'est que peu pacifiée. Au sein de la visibilité technicisée, les ruses sont nombreuses pour avoir une longueur d'avance tant sur les adversaires que sur la modération. Par ailleurs, elles assurent une série de comportements nuisibles et délétères qui valorisent le *spam*, le *trolling* ou encore le harcèlement. Certes, la duperie et la manipulation ont toujours été une composante importante de la propagande (Almeida, 1995 ; Wolton et Wieviorka, 1987), mais les technologies numériques en ont redessiné les contours et le champ de possibilités. Ces actions peuvent être portées par des agents automatisés, qui ciblent massivement d'autres utilisateurs, journalistes et personnalités politiques, dans des formats qui cherchent à provoquer l'émoi chez l'adversaire. Des pratiques déjà observées au sein des militants d'extrême droite (boyd, 2017 ; Marwick et Lewis, 2017). Cela montre que la politique se doit d'être pensée à travers ces associations complexes qui combinent le code et les militants. Nous avons montré que ces alliances peuvent parfois mener à l'échec de la

logique de la contradiction ; en favorisant un univers numérique de plus en plus truqué et polarisé.

Enfin, nous avons montré empiriquement comment la modération fonctionne et constitue un élément majeur des luttes pour la visibilité à l'ère des plateformes numérique. Ainsi, cette composante de la visibilité déborde du champ de l'activisme et pose la question du rôle politique des plateformes. Face à la menace terroriste, les gouvernements ont de plus en plus délégué la modération aux entreprises privées, en faisant du filtrage automatisé la clé d'une censure efficace. Ces dernières années, les grandes plateformes numériques ont intégré à leur architecture des algorithmes de détection automatique qui n'effectuent souvent qu'un premier filtrage. On observe, que dans ces nouvelles reconfigurations de la censure, les gouvernements occupent une place importante, que ce soit par le renforcement de mesures législatives ou encore par la légitimation d'une censure administrative. Par ailleurs, les géants du web opèrent dans la plus grande opacité. Ainsi, la gestion de la censure, et plus largement du problème de terrorisme devient l'objet d'une boîte noire administrée par une poignée d'entreprises privées américaines. Face à cette opacité, cette thèse appelle les entreprises des réseaux sociaux à procéder au difficile travail de transparence et de responsabilité, en rapport avec les algorithmes, les données utilisées et les biais internes. Si des efforts ont pu être constatés en matière de transparence, notamment en raison de nouvelles législations européennes, ils restent pour l'heure extrêmement faibles.

D'un point de vue théorique, notre thèse propose une trame conceptuelle fertile pour étudier la visibilité médiatisée des groupes activistes. Son cadre théorique fait une large place au rôle actif des non-humains, des reconfigurations humains-machines et des dimensions socio-techniques et culturelles des plateformes. Ainsi, si l'insistance sur le rôle des non-humains et sur la configuration humain-machine n'est pas une idée nouvelle, la nouveauté réside dans le fait d'actualiser ces principes dans leur rapport à l'activisme dans sa forme extrémiste. Cela ouvre une nouvelle perspective pour la sociologie des mouvements sociaux, les études en communication et les études sur le terrorisme, qui ont peu pensé le rôle des non-humains et les processus de co-constitution entre militant et technique. Fondée sur une approche relationnelle, notre approche théorique permet de reconstruire la dynamique de visibilité en ligne de groupes extrémistes en envisageant les reconfigurations mutuelles. Cela signifie envisager la visibilité comme le produit de l'imbrication d'une agentivité militante et d'une agentivité technique. Inévitablement, cela place l'analyse de la visibilité en ligne dans une

dynamique du mouvement où les réalités se font et défont constamment. Tout en la replaçant dans son « contexte socio-matériel ».

Par ailleurs, notre étude s'inscrit quelque peu en discontinuité avec l'ANT. Au sein de l'ANT, la violence n'est jamais prise en compte. Cela part du principe qu'il existe « uniquement des rapports de force, qui se traduisent par la victoire des plus forts et l'échec des plus faibles » (Dodier, 1995). Il y a donc bien des forces qui déstabilisent le réseau, mais ces forces ne peuvent se traduire en violence. Cela découle entre autres de son impossibilité à considérer une anthropologie normative. Or, ce qui est entre autres infléchi dans le réseau technico-jihadiste à l'étude, c'est le sens du conflit et de la violence. Cela nous incite à penser la violence qui gouverne les assemblages socio-techniques. L'assemblage ne se limite pas à une histoire d'intérêt, mais peut aussi prendre en charge un langage de la violence et du choc émotionnel. Il y a les récits, mais il y a aussi les actions qui visent à soustraire l'opposant à l'objectif assumé à l'invisibilité. C'est à ces conditions que les assemblages se détachent de l'unique prise en compte des rapports de force qui articulent des stabilités et instabilités au sein des réseaux socio-techniques.

Maintenant que nous avons terminé de détailler nos contributions, il importe d'en expliquer les retombées pratiques potentielles. Notre thèse permet de mieux comprendre un enjeu majeur de notre temps, celui de la propagation de discours extrémistes en ligne, plus particulièrement la propagande jihadiste. Cette diffusion a particulièrement inquiété les pouvoirs publics et la société civile, notamment à la faveur du nombre de jeunes partis faire le jihad et de la multiplication des attentats commis en Occident. Notre thèse offre ainsi un éclairage inédit sur le fonctionnement de la propagande jihadiste en ligne, la modération et les capacités de résistance du groupe jihadiste face à la censure. Ces enjeux sont majeurs. En les envisageant dans le détail, notre thèse est susceptible d'informer les décideurs dans l'élaboration de politiques de sécurité avisées.

Pistes pour des recherches futures

À l'issue de ce travail, plusieurs pistes de recherches ont émergé. Nous mentionnerons brièvement deux axes de recherches qui nous semblent importants à privilégier pour bonifier nos connaissances sur les processus contemporains de visibilités à des fins politiques.

Premièrement, il s'agirait de mettre à l'épreuve notre proposition de « visibilité technicisée » en étudiant comment d'autres groupes radicaux manipulent les plateformes numériques pour propager leur propagande. Les usages que nous avons observés sont-ils transposables à d'autres groupes ? Ces formes de visibilité sont-elles globales ? Cette forme de visibilité concerne-t-elle d'autres formations politiques ou est-elle spécifique aux groupes extrémistes ? Nous pouvons d'ores et déjà noter que le maniement de l'écosystème numérique pour manipuler l'opinion attise l'intérêt des chercheurs depuis quelques années maintenant (par exemple Abokhodair et al., 2015 ; Benkler et al., 2018 ; Howard et al., 2016 ; Howard et Kollanyi, 2016 ; Marwick et Lewis, 2017).

Par ailleurs, certains groupes restent exclus de ce champ de recherche, notamment les groupes d'extrême gauche ou encore d'autres groupes jihadistes. Dans un contexte où les technologies numériques deviennent ubiquitaire dans la plupart des processus politiques, il serait pertinent de dresser les similitudes et les différences dans les processus d'apparence publique à l'ère du numérique. De plus, étendre notre proposition à d'autres cas permettrait de souligner d'autres tactiques qui cherchent à manipuler l'opinion. Cela est d'autant plus pertinent face au développement toujours croissant des nouvelles technologies et de l'intelligence artificielle. Une pratique telle que le *deepfake* constitue un exemple récent de manœuvre manipulatoire. Cette technique consiste à superposer des fichiers existants (audio et vidéo) sur d'autres vidéos. Ces pratiques qui reposent sur des méthodes d'intelligence artificielle risquent d'altérer le paysage politique en élargissant l'horizon des fausses informations. Enfin, il s'agirait de prolonger la réflexion concernant les nouvelles formes de domination et d'asymétrie qui sont subséquentes à ces formes de visibilités technicisées.

Deuxièmement, notre recherche ouvre de nouvelles perspectives sur la relation entre machine et humain. Notre cas fait figure d'exemple face à un phénomène qui se propage depuis plusieurs années, à savoir le déploiement de *botnets* politiques. L'implication des *botnets* dans les processus politiques est une question sociologiquement importante. Elle soulève la question difficile des bouleversements qui affectent les questions politiques. Plusieurs questions que nous n'avons pu traiter dans notre étude mériteraient d'être approfondies. La première est celle qui concerne la relation entre les *botnets* et les autres utilisateurs. Les *botnets* créent-ils des changements significatifs dans les conversations ? Quelles sont les représentations que le public se fait de ces agents automatisés ? Existe-t-il un ajustement en fonction de la représentation de l'artificialité de l'interlocuteur ? Un deuxième axe concerne

les scripts et les concepteurs de ces *botnets*. Il s'agit cette fois-ci de porter un intérêt sur les processus de fabrications et les promesses faites derrière ces agents automatisés. Comment ces logiciels sont négociés dans un réseau d'acteurs humains et non-humains ? Quels sont les objectifs donnés à ces technologies par les utilisateurs ou les États qui les développent ? Comment les développeurs imaginent les promesses et les pouvoirs des *botnets* politiques ? Une autre piste intéressante concerne également la responsabilité des compagnies qui profitent du trafic des agents automatisés. Comment assurer des mécanismes de transparence et de responsabilité face au déploiement de *botnets* dans des processus politiques ? Est-ce que les plateformes numériques ont une responsabilité à avoir dans la facilitation de l'identification des comptes gérés par des *botnets* ? Par exemple, nous avons vu lors de notre enquête que contrairement à Twitter, Telegram est plus transparent envers son audience en ce qui concerne les *botnets*. La plateforme prévoit entre autres que chaque compte géré par ces agents automatisés soit joint de la mention *botnet* .

Bibliographie

Abokhodair, N., Yoo, D., & McDonald, D. W. (2016). Dissecting a social botnet: Growth, content and influence in Twitter. Dans *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (p. 839-851). Repéré à https://arxiv.org/abs/1604.03627.

Adams, P. C. (1997). Cyberspace and virtual places. *Geographical Review* 87:155–71.

Adelman, R. A. (2018). One apostate run over, hundreds repented: excess, unthinkability, and infographics from the war with ISIS. *Critical Studies in Media Communication*, *35*(1), 57-73.

Akrich, M. (1989). La construction d'un système socio-technique. Esquisse pour une anthropologie des techniques. *Anthropologie et sociétés*, *13*(2), 31-54.

Akrich, M. (1990). De la sociologie des techniques à une sociologie des usages. *Techniques et culture*, *16*, 83-110.

Akrich M., (1992). The de-scription of technical objects. Dans W. Bijker et J. Law (dir.), *Shaping Technology/Building Society* (p. 205-224). Cambridge, MA : MIT Press.

Akrich, M. (1993). Les formes de la médiation technique. *Réseaux*, (60), 87-98.

Akrich, M. (1994). Comment sortir de la dichotomie technique/société. Dans B. Latour et P. Lemonnier (dir.). *De la préhistoire aux missiles balistiques : l'intelligence sociale des techniques* (p. 105-131). Paris : La Découverte.

Akrich, M. (1995). User representations: Practices, methods and sociology. Dans A. Rip et T. Misa et J. Schot, *Managing technology in Society* (p. 167-184). Pinter Publishers : London.

Akrich, M. (2006). Les objets techniques et leurs utilisateurs. De la conception à l'action. Dans M. Callon, B. Latour et M. Akrich (dir.), *Sociologie de la traduction. Textes fondateurs* (p. 179-199). Paris : Presses des Mines.

Akrich, M. (2010). Comment décrire les objets techniques?. *Techniques & Culture. Revue semestrielle d'anthropologie des techniques, (54-55),* 205-219.

Akrich, M., & Boullier, D. (1991). Le mode d'emploi : genèse, forme et usage. Dans D. Chevallier (dir.), *Savoir faire et pouvoir transmettre* (p. 113-131). Paris : Éditions de la Maison des sciences de l'homme

Akrich, M., & Latour, B. (1992). A summary of a convenient vocabulary for the semiotics of human and nonhuman assemblies. Dans W. Bijker et J. Law (dir.), *Shaping Technology/Building Society* (p. 259-264). Cambridge, MA : MIT Press.

Akrich, M., & Méadel, C. (2007). De l'interaction à l'engagement : les collectifs électroniques, nouveaux militants de la santé. *Hermès, La Revue*, (1), 145-153.

Aktypi, M. (2012). Donna Haraway et les technologies de l'ordinaire. Dans E. Dorlin et E. Rodriguez (dir.), *Penser avec Donna Haraway* (p. 103-123). Paris : PUF.

Albert, P. (2010). *Histoire de la presse. Que sais-je ?* Paris : PUF.

Allen, M. (2013). What was Web 2.0? Versions as the dominant mode of internet history. *New Media & Society*, *15*(2), 260-275.

Almeida, F. (1995). *Images et propagande*. Paris: Casterman.

Aminzade, R., & McAdam, D. (2001). Emotions and Contentious Politics. Dans R. . Aminzade, J. A. Goldstone, D. McAdam, E. J. Perry, W. H. Sewell, S. Tarrow et C. Tilly (dir.), *Silence and Voice in the Study of Contentious Politics* (p. 14-50). New York : Cambridge University Press.

Ananny, M. (2016). Toward an ethics of algorithms: Convening, observation, probability, and timeliness. *Science, Technology, & Human Values*, *41*(1), 93-117.

Anderson, C. W. (2011). Deliberative, agonistic, and algorithmic audiences: Journalism's vision of its public in an age of audience transparency. *International Journal of Communication*, *5*, 19.

Arendt, H. (1961). *Condition de l'homme moderne*. Paris : Pocket.

Arendt, H. (1972). *Du mensonge à la violence : essais de politique contemporaine*. Paris : Pocket.

Arendt, H. (1995). *Qu'est-ce que la politique?*. Paris : Edition du Seuil.

Arquilla, J., & Ronfeldt, D. F. (2002). Netwar revisited: the fight for the future continues. *Low Intensity Conflict & Law Enforcement*, *11*(2-3), 178-189.

Ayres, J. M. (1999) From the streets to the Internet: the cyber-diffusion of contention. *The Annals of the American Academy of Political and Social Science,566*, 132–143.

Atran, S. (2016). *L'État islamique est une révolution*. Paris : Les liens qui libèrent.

Atwan, A. B. (2015). *Islamic state: The digital caliphate*. Berkeley, CA : Univiversity of California Press.

Awan, A. N. (2007a). Radicalization on the Internet? The virtual propagation of jihadist media and its effects. *The RUSI Journal*, *152*(3), 76-81.

Awan, A. N. (2007b). Virtual jihadist media Function, legitimacy and radicalizing efficacy. *European Journal of Cultural Studies*, *10*(3), 389-408.

Awan, I. (2017). Cyber-extremism: Isis and the power of social media. *Society*, *54*(2), 138-149.

Backes, U. (2007). Meaning and Forms of Political Extremism in Past and Present. *Středoevropské politické studie*, *9*(4), 242-262.

Badouard, R. (2013). Les mobilisations de clavier. *Réseaux*, (5), 87-117.

Badouard, R. (2014). La mise en technologie des projets politiques. Une approche « orientée design » de la participation en ligne. *Participations*, (1), 31-54.

Barad, K. (2007). *Meeting the universe halfway: Quantum physics and the entanglement of matter and meaning*. Durham, NC : Duke University Press.

Barbier, R., & Trépos, J. Y. (2007). Humains et non-humains : un bilan d'étape de la sociologie des collectifs. *Revue d'anthropologie des connaissances*, *1*(1), 35-58.

Barnet, B. A. (2009). Idiomedia: The rise of personalized, aggregated content. *Continuum*, *23*(1), 93-99.

Barthes, R. (1957). *Mythologies*. Paris : Le Seuil.

Barus-Michel, J. (2011). Une société sur écrans. Dans N. Aubert & C. Haroche (dir.), *Les tyrannies de la visibilité : Être visible pour exister ?* (p. 25-29). Toulouse : Érès.

Barzilai-Nahon, K., & Neumann, S. (2005). Bounded in cyberspace: An empirical model of self-regulation in virtual communities. Dans *Proceedings of the 38th Annual Hawaii International Conference on System Sciences.* Repéré à https://ieeexplore.ieee.org/abstract/document/1385627

Batty, M. (1993). The geography of cyberspace. *Environment and Planning B: Planning and Design* 20, 615-61.

Baudrillard, J. (1981). *Simulacres et Simulation*. Paris : Éditions Galilée.

Baudrillard, J. (2004). *La violence faite aux images*. Conférence ENS, Paris. Repéré à : https://www.academia.edu/10874952

Baugut, P., & Neumann, K. (2019). How right-wing extremists use and perceive news media. *Journalism & Mass Communication Quarterly*, *96*(3), 696-720.

Baym, N. K. (1995). The emergence of community in computer-mediated communication. Dans S. G. Jones (dir.), *CyberSociety : Computer-mediated communication and community* (p. 138-163). Thousand Oaks, CA : Sage Publications.

Baym, N.K. (2000). *Tune In, Log On : Soaps, Fandom and Online Community*. Thousand Oaks, CA : Sage.

Baym, N. K., & Markham, A. N. (2009). Introduction : Making smart choices on shifting ground. Dans A. Markham et N. Baym (dir.), *Internet inquiry : Conversations about method* (p. vii-xix). Thousand Oaks, CA : SAGE.

Beaulieu, A. (2004). Mediating ethnography: objectivity and the making of ethnographies of the internet. *Social epistemology*, *18*(2-3), 139-163.

Beaulieu, A., & Estalella, A. (2012). Rethinking research ethics for mediated settings. *Information, Communication & Society*, *15*(1), 23-42.

Becker, H. S. (2007). *Les ficelles du métier : comment conduire sa recherche en sciences sociales*. Paris : La Découverte.

Beer, D. (2009). Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society*, *11*(6), 985-1002.

Beer D. (2017). The social power of algorithms. *Information, Communication & Society*, 20(1), 1-13.

Beer, D., & Burrows, R. (2007). Sociology and, of and in Web 2.0: Some initial considerations. *Sociological research online*, *12*(5), 1-13.

Benedikt, M. (1991). *Cyberspace: first steps*. Cambridge, MA: MIT Press.

Benford, R. D. (1993). Frame disputes within the nuclear disarmament movement. *Social forces*, *71*(3), 677-701.

Benford, R. D. (1997). An insider's critique of the social movement framing perspective. *Sociological inquiry*, *67*(4), 409-430.

Benford, R. D., & Snow, D. A. (2000). Framing processes and social movements: An overview and assessment. *Annual review of sociology*, *26*(1), 611-639.

Benford, R. D., Snow, D. A. (2012). Processus de cadrage et mouvements sociaux : présentation et bilan. *Politix*, (3), 217-255.

Benhamou, B. (2002). Les enjeux politiques de l'architecture et de la régulation de l'internet. *Les Cahiers du numérique*, *3*(2), 197-212.

Benjamin, W. (1963). *Œuvres III*. Paris : Gallimard.

Benkler, Y. (2009). *La richesse des réseaux : marchés et libertés à l'heure du partage social* (A. Clerq-Roques, M. Lahache, B. Coing, L. Duval, A. Bouillon & Pierre Bouillon, Trad.). Lyon : Presses Universitaires de Lyon.

Benkler, Y., Faris, R., & Roberts, H. (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford : Oxford University Press.

Bennett, W. L., Breunig, C., & Givens, T. (2008). Communication and political mobilization: Digital media and the organization of anti-Iraq war demonstrations in the US. *Political communication*, *25*(3), 269-289.

Bennett, W. L. & Segerberg A. (2012) The logic of connective action. *Information, Communication & Society* 15(5): 739–768.

Benotman, N., & Malik, N. (2016). The Children of Islamic State. *The Quilliam Foundation.* Repéré à https://f.hypotheses.org/wp-content/blogs.dir/2725/files/2016/04/the-children-of-islamic-state.pdf

Berger, J. M., & Morgan, J. (2015). The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter. *The Brookings Project on US Relations with the Islamic World*, *3*(20), 4-1. Repéré à https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.

Berry, V. (2012). Ethnographie sur Internet : rendre compte du «virtuel». *Les Sciences de l'éducation-Pour l'Ère nouvelle*, *45*(4), 35-58.

Berry, D. (2016). *The philosophy of software: Code and mediation in the digital age*. Berlin : Springer.

Bessi, A., & Ferrara, E. (2016). Social bots distort the 2016 US Presidential election online discussion. *First Monday*, 21(11).

Bigo, D. (2005). L'impossible cartographie du terrorisme. *Cultures & conflits* [En ligne]. Repéré à https://journals.openedition.org/conflits/1149?lang=es

Bijker, W. E., Hughes, T. P., & Pinch, T. J. (dir.). (1987). *The social construction of technological systems: New directions in the sociology and history of technology*. Cambridge, MA: MIT Press.

Bimber, B. (2001). Information and political engagement in America: The search for effects of information technology at the individual level. *Political Research Quarterly*, *54*(1), 53-67.

Bimber B (2003) *Information and American Democracy: Technology in the Evolution of Political Power*. Cambridge: Cambridge University Press.

Bingham, N. (1996). Object-ions: from technological determinism towards geographies of relations. *Environment and Planning D: Society and Space*, *14*(6), 635-657.

Blaker, L. (2015). The Islamic State's use of online social media. *Military Cyber Affairs*, *1*(1), 4.

Bleil, S. (2005). Avoir un visage pour exister publiquement : l'action collective des sans terre au bresil. *Réseaux*, (1), 123-153.

Bloom, M., Tiflati, H., & Horgan, J. (2019). Navigating ISIS's preferred platform: Telegram1. *Terrorism and Political Violence*, *31*(6), 1242-1254.

Bockstette, C. (2009). Taliban and Jihadist terrorist use of strategic communication. *Connections*, *3*(8), 1-24.

Boellstorff, T. (2015). *Coming of age in Second Life: An anthropologist explores the virtually human*. Princeton, NJ : Princeton University Press.

Bogerts, L., & Fielitz, M. (2018). Do You Want Meme War? Dans M. Fielitz et N. Thruston (dir.), *Post-Digital Cultures of the Far Right* (p. 137-153). Bielefeld : Transcript Verlag.

Bolt, N. (2012). *Insurgent propaganda and the new revolutionaries.* New York, NY : Columbia University Press.

Boltanski, L. (1990). *L'amour et la justice comme compétences : trois essais de sociologie de l'action*. Paris : Métailié.

Boltanski, L., & Thévenot, L. (1991). *De la justification : Les économies de la grandeur.* Paris : Gallimard.

Bonditti, P. (2005). Biométrie et maîtrise des flux : vers une «géo-technopolis du vivant-en-mobilité»?. *Cultures & Conflits*, (58), 131-154.

Bonilla, Y., & Rosa, J. (2015). # Ferguson: Digital protest, hashtag ethnography, and the racial politics of social media in the United States. *American Ethnologist*, *42*(1), 4-17.

Boumaza, M., & Campana, A. (2007). Enquêter en milieu «difficile». *Revue française de science politique*, *57*(1), 5-25.

Boullier, D. (2012). Preserving diversity in social networks architectures. Dans F. Massit-Folléa, C. Maédel et L. Monnoyer-Smith (dir.), *Normative Experience in Internet Politics* (p. 187-209). Paris : Presses des Mines.

Boullier, D. (2016). *Sociologie du numérique*. Malakoff : Armand Colin.

Bourdieu, P. (1996). *Sur la télévision : suivi de L'emprise du journaliste*. Paris : Raison d'agir.

boyd, D. (2009). How can qualitative internet researchers define the boundaries of their projects: A response to Christine Hine. Dans A. Markham et N. Baym (dir.), *Internet inquiry : Conversations about method* (p.26-32). Thousand Oaks, CA : SAGE.

boyd, D. (2014). *It's complicated: The social lives of networked teens*. New Haven, CT : Yale University Press.

boyd, D. (2017). Hacking the attention economy. *Data & Society*. Repéré à https://points. datasociety. net/hacking-the-attention-economy-9fa1daca7a37.

boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, communication & society*, *15*(5), 662-679.

Brachman, H. (2009). *Global Jihadism : Theory and Practice*. Abingdon : Routledge.

Brachten, F., Stieglitz, S., Hofeditz, L., Kloppenborg, K., & Reimann, A. (2017). Strategies and Influence of Social Bots in a 2017 German state election-A case study on Twitter. Dans *Proceedings of the Australasian Conference on Information Systems* (p.1-12). Repéré à https://arxiv.org/pdf/1710.07562v1.pdf.

Braun, E. (2017 ; 31 octobre). Google, Facebook et Twitter dans la tourmante de « l'enquête russe ». *Le Figaro*. Repéré à http://www.lefigaro.fr/secteur/high-tech/2017/10/11/32001-20171011ARTFIG00271-google-facebook-et-twitter-dans-la-tourmente-de-l-enquete-russe.php.

Breteau (2019, 26 mars). L'État islamique en 58 cartes. *Le Monde*. Repéré à https://www.lemonde.fr/les-decodeurs/article/2019/03/26/l-ei-en-58-cartes-de-la-proclamation-du-califat-a-la-fin-de-l-emprise-territoriale_5441495_4355770.html

Brighenti, A. (2007). Visibility: A category for the social sciences. *Current sociology*, *55*(3), 323-342.

Brighenti, A. M. (2010). *Visibility in social theory and social research*. London : Palgrave Macmillan.

Bromseth, J. C. (2002). Public places–public activities. Dans A. Morrison (dir.), *Researching ICTS in Contexte* (p.33-63). InterMedia Report University of Oslo. Repéré à https://pdfs.semanticscholar.org/a2a5/8e6ea6dcd7906b0317e54e580db98d256cde.pdf

Brousseau, E. & Curien, N. (2001). Économie d'Internet, économie du numérique. *Revue économique*, *7,* (52), 7-36.

Brousseau, E., Marzouki, M. & Méadel, C. (2012). Governance, networks and digital technologies : societal, political and organizational innovations. Dans E. Brousseau, M. Marzouki & C. Méadel (dir.), *Governance, Regulations and Powers on the Internet* (p. 3-39). Cambridge : Cambridge University Press.

Brundidge, J. (2010). Encountering "difference" in the contemporary public sphere: The contribution of the Internet to the heterogeneity of political discussion networks. *Journal of Communication*, *60*(4), 680-700.

Buchanan, E (2010). Internet research ethics: past, present and future. Dans M. Consalvo & C. Ess (dir.), *The Handbook of Internet Studies* (p. 88-103). Chichester: Blackwell Publishing.

Bucher, T. (2012). Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. *New media & society*, *14*(7), 1164-1180.

Bucher, T. (2018). *If... then: Algorithmic power and politics*. Oxford : Oxford University Press.

Burgess, J. & Green, J. (2009). *YouTube*. Cambridge: Polity Press.

Burke, J. (2016). The age of selfie jihad: How evolving media technology is changing terrorism. *CTC Sentinel*, *9*(11), 1-8.

Burrell, J. (2009). The field site as a network: A strategy for locating ethnographic research. *Field methods*, *21*(2), 181-199.

Burrell, J. (2016). How the machine “thinks”: Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1), 2053951715622512.

Burris, V., Smith, E., & Strahm, A. (2000). White supremacist networks on the Internet. *Sociological focus*, *33*(2), 215-235.

Buton, P. (2003). L'adieu aux armes?. *Vingtième siècle. Revue d'histoire*, (4), 43-54.

Buton, P. (2013). L’iconographie révolutionnaire en mutation. *Cultures & Conflits*, (91/92), 31-44.

Byman, D. (2016). Understanding the Islamic state—A review essay. *International Security*, *40*(4), 127-165.

Caiani, M., & Parenti, L. (2009). The dark side of the web: Italian right-wing extremist groups and the Internet. *South European Society and Politics*, *14*(3), 273-294.

Caiani, M., & Parenti, L. (2011). The Spanish extreme right and the Internet. *Análise social*, 46(201), 719-740.

Caiani, M., & Wagemann, C. (2009). Online networks of the Italian and German extreme right: An explorative study with social network analysis. *Information, Communication & Society*, *12*(1), 66-109.

Callon, M. (1979). L’État face à l’innovation technique : le cas du véhicule électrique. *Revue française de science politique*, 426-447.

Callon, M. (1986). Éléments pour une sociologie de la traduction : la domestication des coquilles Saint-Jacques et des marins-pêcheurs dans la baie de Saint-Brieuc. *L’Année sociologique (1940/1948-)*, *36*, 169-208.

Callon, M. (1987). Society in the making: the study of technology as a tool for sociological analysis. Dans W. E. Bijker, T. P. Hughes et T. Pinch (dir.), *The social construction of technological systems: New directions in the sociology and history of technology* (p. 83-103). Cambridge, MA : MIT Press.

Callon M. (dir.) (1989), *La Science et ses réseaux. Genèse et circulation des faits scientifiques, Anthropologie des sciences et des techniques.* Paris : La Découverte.

Callon, M. (1991). Réseaux technico-économiques et irréversibilité. Dans R. Boyer, B. Chavance & O. Godard (dir.), *Les figures de l’irréversibilité en économie* (p. 195-233). Paris : Éditions de l’EHESS.

Callon, M. (2006). Sociologie de l’acteur réseau. Dans M. Callon, B. Latour et M. Akrich (dir.), *Sociologie de la traduction. Textes fondateurs* (p. 267-276). Paris : Presses des Mines.

Callon, M., & Latour, B. (1981). Unscrewing the big Leviathan: how actors macro-structure reality and how sociologists help them to do so. Dans K. Knorr Cetina et A.V. Cicourel

(dir.), *Advances in social theory and methodology: Toward an integration of micro-and macro-sociologies* (p. 277-304). London & New York : Routledge.

Callon, M., Lascoumes, P., & Barthe, Y. (2001). *Agir dans un monde incertain : essai sur la démocratie technique*. Paris : Seuil.

Callon, M., & Latour, B. (1992). Don't throw the baby out with the bath school! A reply to Collins and Yearley. *Science as practice and culture*, *343*, 368.

Callon, M., & Law, J. (1997). L'irruption des non-humains dans les sciences humaines : quelques leçons tirées de la sociologie des sciences et des techniques. Dans B. Reynaud (dir.), *Les limites de la rationalité. Tome 2* (p. 99-118). Paris : La Découverte.

Callon, M., & Muniesa, F. (2003). Les marchés économiques comme dispositifs collectifs de calcul. *Réseaux*, (6), 189-233.

Cammaerts, B. (2008). Critiques on the participatory potentials of Web 2.0. *Communication, culture & critique*, *1*(4), 358-377.

Camus, A. (1942). Le Mythe de Sisyphe. Paris : Le Seuil

Cardon, D. (2009). Le design de la visibilité. *Réseaux*, (6), 93-137.

Cardon, D. (2010). *La démocratie Internet : Promesses et limites.* Paris : Le Seuil.

Cardon, D. (2011). Le parler privé-public des réseaux sociaux d'Internet. Dans S. Proulx, M. Millette & L. Heaton (dir.), *Médias sociaux : enjeux pour la communication* (pp.33-47). Québec : Presses de l'Université du Québec.

Cardon, D. (2015). *À quoi rêvent les algorithmes : Nos vies à l'heure des big data*. Paris : Le Seuil.

Cardon, D. (2019). *Culture numérique*. Paris : Presses de Sciences Po.

Cardon, D. & Casilli, A. (2015). *Qu'est-ce que le digital labor ?* Paris : Éditions INA.

Cardon, D., & Granjon, F. (2010). *Médiactivistes.* Paris : Presses de Sciences Po.

Cardoso, G. (2012). Networked life world: Four dimensions of the cultures of networked belonging. *Observatorio*, 197-205.

Cardoso, G. & Pereira, P. N. (2004). Mass media driven mobilization and online protest: ICTs and the pro-East Timor movement in Portugal. Dans W. Van de Donk, B.D. Loader, P.G. Nixon & D. Rucht (dir.) *Cyberprotest: New Media, Citizens and Social Movements* (p.147-168). London & New York : Routledge.

Carey, J. (1989) *Communication as Culture: Essays on Media and Society.* London : Unwin Hyman.

Carroll, W. K., & Hackett, R. A. (2006). Democratic media activism through the lens of social movement theory. *Media, culture & society*, *28*(1), 83-104.

Casilli, A. A. (2017). Global Digital Culture| Digital Labor Studies Go Global: Toward a Digital Decolonial Turn. *International Journal of Communication*, *11*, 21

Casilli, A. (2018). La plateformisation comme mise au travail des usagers. Dans B. Coriat, N. Alix, J.-L. Bancel et F. Sultant (dir.), *Vers une République des Biens Communs ?, Les Liens qui Libèrent*, (p. 41-56). Paris : Les liens qui libèrent.

Castells, M. (1998). *La société en réseaux* (Vol. 1) (traduit par P. Delamare). Paris : Fayard.

Castells, M. (2000). Materials for an exploratory theory of the network society1. *The British journal of sociology*, *51*(1), 5-24.

Castells, M. (2007). Communication, power and counter-power in the network society. *International journal of communication*, *1*(1), 29.

Castells, M. (2009). *Communication power*. Oxford : Oxford University Press.

Cefaï, D. (2016). Publics, problèmes publics, arènes publiques…. *Questions de communication*, (2), 25-64.

Cefaï, D., & Pasquier, D. (2003). *Les sens du public*. Paris : PUF

Chadwick, A., 2017. *The hybrid media system: politics and power*. Oxford: Oxford University Press.

Chadwick, A., & Howard, P. N. (dir.). (2010). *Routledge handbook of Internet politics*. Abingdon-on-Thames : Taylor & Francis.

Chalfont, L., Soustelle, J., Podhoretz, N., Lowenthal, G., Will, G., & Elkins, M. (1980). Political violence and the role of the media: Some perspectives. *Political Communication*, *1*(1), 79-99.

Chaliand, G. (2015). Le jihadisme à l'heure de Daech. Dans G. Chaliand et A. Blin (dir.), *Histoire du terrorisme : de l'Antiquité à Daech* (p.643-665). Villeneuve-d'Ascq : Fayard.

Chaliand, G., & Blin, A. (2015). *Histoire du terrorisme : de l'antiquité à Al Qaida*. Villeneuve-d'Ascq : Fayard.

Chambers, S., & Costain, A. (dir.). (2000). *Deliberation, democracy, and the media*. Lanham, MD : Rowman & Littlefield Publishers.

Champagne, P. (1984). La manifestation. La production de l'événement politique. *Actes de la recherche en sciences sociales*, *52*(1), 19-41.

Champagne, P. (1990). *Faire l'opinion : le nouveau jeu politique*. Editions de Minuit : Paris.

Champagne, P. (1991). La construction médiatique des malaises sociaux. *Actes de la recherche en sciences sociales*, *90*(1), 64-76.

Cheney-Lippold, J. (2018). *We are data: Algorithms and the making of our digital selves*. New York, NY : NYU Press.

Chermak, S. M., & Gruenewald, J. (2006). The media's coverage of domestic terrorism. *Justice Quarterly*, *23*(4), 428-461.

Christensen, H. S. (2011). Political activities on the Internet: Slacktivism or political participation by other means?. *First Monday*, *16*(2).

Christou G and Simpson S (2009) New governance, the Internet, and country code top-level domains in Europe. *Governance: An International Journal of Policy Administration and Institutions, 22*, 599–624.

Chouliaraki, L., & Kissas, A. (2018). The communication of horrorism: A typology of ISIS online death videos. *Critical Studies in Media Communication*, *35*(1), 24-39.

Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2010, December). Who is tweeting on Twitter: human, bot, or cyborg?. Dans *Proceedings of the 26th annual computer security applications conference* (p. 21-30). Repéré à https://www.eecis.udel.edu/~hnw/paper/acsac10.pdf.

Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2012). Detecting automation of twitter accounts: Are you a human, bot, or cyborg?. Dans *IEEE Transactions on Dependable and Secure Computing*, *9*(6), 811-824. Repéré à https://ieeexplore.ieee.org/document/6280553.

Chun, W. H. K. (2005). On software, or the persistence of visual knowledge. *Grey room*, 26-51.

Chun, W. H. K. (2011a). *Programmed visions: Software and memory*. Cambridge, MA : MIT Press.

Chun, W. H. K. (2011b). Crisis, crisis, crisis, or sovereignty and networks. *Theory, Culture & Society*, *28*(6), 91-112.

Citron, D. K. (2014). *Hate crimes in cyberspace*. Cambridge : Harvard University Press.

Citron, D. K. (2018). Extremist speech, compelled conformity, and censorship creep. *Notre Dame L. Rev.*, *93*, 1035-1072.

Citton, Y. (dir.). (2014). *L'économie de l'attention : nouvel horizon du capitalisme?*. Paris : La Découverte.

Classen, C. (1993). *Worlds of Sense : Exploring the Senses in History and Across Cultures*. London & New York : Routledge.

Classen, C. (1997). Foundations for an anthropology of the senses. *International Social Science Journal*, *49*(153), 401-412.

Cohen, S. (1972). *Folk devils and moral panics: The creation of the mods and rockers*. St Alban : Granada Publishing Limited.

Cole, J. (2012). Radicalisation in virtual worlds: Second Life through the eyes of an avatar. *Journal of Policing, Intelligence and Counter Terrorism*, *7*(1), 66-79.

Coleman, E. G. (2010). Ethnographic approaches to digital media. *Annual review of anthropology*, *39*, 487-505.

Coleman, G. (2011). Hacker politics and publics. *Public Culture*, *23*(3 (65), 511-516.

Coleman, G. (2016). *Anonymous : hacker, activiste, faussaire, mouchard, lanceur d'alerte*. Montréal : Lux Éditeur.

Como, D. R. (2007). Secret printing, the crisis of 1640, and the origins of civil war radicalism. *Past and Present*, *196*(1), 37-82.

Conein, B., Dodier, N., & Thévenot, L. (1993). *Les objets dans l'action : De la maison au laboratoire*. Paris : Raisons pratiques.

Contamin, J.G. (2010). Cadrages et luttes de sens. Dans E. Agrikoliansky, I. Sommier et O. Fillieule, *Penser les mouvements sociaux* (p.55-75). Paris : La Découvete.

Convery, I., & Cox, D. (2012). A review of research ethics in internet-based research. *Practitioner Research in Higher Education*, *6*(1), 50-57.

Conway, M. (2007). Cyberterrorism: Hype and reality. *Computer Freud & Security*, *2007*(2), 9-12.

Conway, M. (2012). From al-Zarqawi to al-Awlaki: The Emergence of the Internet as a new form of violent radical milieu. *Combating Terrorism Exchange*, *2*(4), 12-22.

Conway, M. (2014). From « cyberterrorism » to « online radicalism ». Dans M. Eid (dir.) *Exchanging terrorism oxygen for media airwaves : The Age of Terredia* (p.198-217). Hershey, PA : IGI Global.

Cook, D. (2017). Contemporary Martyrdom : Ideology and Material Culture. Dans T. Hegghammer (dir.). *The Art and Social Practices of Militant Islamists* (p.151-171). Cambridge : Cambridge University Press.

Cormode, G., & Krishnamurthy, B. (2008). Key differences between Web 1.0 and Web 2.0. *First Monday*, *13*(6).

Costanza-Chock, S. (2003). Mapping the repertoire of electronic contention. *Contributions To The Study Of Mass Media And Communications*, *66*, 173-191.

Cotter, K. (2019). Playing the visibility game: How digital influencers and algorithms negotiate influence on Instagram. *New Media & Society*, *21*(4), 895-913.

Couldry, N. (2015). The myth of "us": digital networks, political change and the production of collectivity. *Information, Communication & Society*, *18*(6), 608-626.

Cramer, F. (2008). Language. Dans M. Fuller (dir.), *Software sutdies/ a lexicon* (p.149-153). Cambridge, MA : MIT Press.

Crelinsten, R. D. (1989). Terrorism and the media: Problems, solutions, and counterproblems. *Political Communication*, *6*(4), 311-339.

Crettiez, X. (2010). Introduction. Penser la violence politique. Dans X. Crettiez et L. Mucchielli (dir.), *Les violences politiques en Europe* (p.7-28). Paris : La découverte.

Crettiez, X. (2013a). Récits et cadrages politiques en Euskadi : lectures de l'iconographie abertzale. *Cultures & Conflits*, (91/92), 81-100.

Crettiez, X., & Piazza, P. (2013b). Iconographies rebelles. Sociologie des formes graphiques de contestation. *Cultures & Conflits*, (91/92), 7-11.

Crettiez, X., & Piazza, P. (2013). Sociologie d'une conversation silencieuse. Protestation iconographique nationaliste et réception publique en Corse. *Cultures & Conflits*, (91/92), 101-121.

Crosset, V., & Dupont, B. (2018). Internet et propagande jihadiste : la régulation polycentrique du cyberespace. *Critique internationale*, (1), 107-125.

Dahlberg, L. (2001). Democracy via cyberspace: Mapping the rhetorics and practices of three prominent camps. *New media & society*, *3*(2), 157-177.

Dahlberg, L. (2007a). Rethinking the fragmentation of the cyberpublic: from consensus to contestation. *New media & society*, *9*(5), 827-847.

Dahlberg, L. (2007b). Dahlberg, L. (2007). The internet and discursive exclusion: From deliberative to agonistic public sphere theory. Dans Dahlberg (dir.), *Radical democracy and the Internet* (p. 128-147). London : Palgrave Macmillan.

Dahlberg-Grundberg, M. (2016). Technology as movement: On hybrid organizational types and the mutual constitution of movement identity and technological infrastructure in digital activism. *Convergence*, *22*(5), 524-542.

Danet, B. (2001). *Cyberpl@y. Communicating online*. Oxford & New York: Berg.

Dauber, C. E., & Robinson, M. (2015). ISIS and the Hollywood visual style. *Jihadology. net*.

David, P. A. (1986). Understanding the economics of QWERTY: The necessity of history. *Economic History and the modern economics*, 30-49.

Dawkins, R. (1976). *The Selfish Gene*. Oxford : Oxford University Press.

Debord, G. (1968). *La société du spectacle*. Paris : Gallimard.

Debord, G., & Wolman, G. J. (2004). Mode d'emploi du détournement. *Inter*, (117), 23-26. [Œuvre originale publiée en 1956]

Debray, R. (1991). *Cours de médiologie générale*. Paris : Gallimard.

De Certeau, M. (1990). *L'invention du quotidien : Arts de faire*. Paris: Gallimard.

De Koster, W., & Houtman, D. (2008). "STORMFRONT IS LIKE A SECOND HOME TO ME" On virtual community formation by right-wing extremists. *Information, Communication & Society*, *11*(8), 1155-1176.

DeLanda, M. (2006). Deleuzian social ontology and assemblage theory. Dans M. Fuglsang et B. Meier Sorensen (dir.), *Deleuze and the Social* (p.250-266). Edinbugh : Edinbugh University Press.

Deleuze, G. (1986). *Foucault*. Paris : Éditions de Minuit.

Deleuze, G., & Guattari, F. (1980). *Mille plateaux : Capitalisme et schizophrénie, 2*. Paris : Éditions de Minuit.

Deleuze, G., & Parnet, C. (2007). *Dialogues II*. New York, NY : Columbia University Press.

Della Porta, D. (1995). *Social Movements, Political Violence, and the State*. Cambridge : Cambridge University Press.

Della Porta, D., & Mosca, L. (2005). Global-net for global movements? A network of networks for a movement of movements. *Journal of Public Policy*, *25*(1), 165-190.

Della Porta, D. (2010). Mouvements sociaux et violence politique. Dans X. Crettiez et L. Mucchielli (dir.), *Les violences politiques en Europe* (p.271-291). Paris : La découverte.

Delmas, R. (2002). Introduction. *Les Cahiers du numérique*, *3*(2), 9-14.

DeNardis, D. (2010). The emerging field of Internet governance. *Yale Information Society Project Working Paper Series*. Repéré à https://auislandora.wrlc.org/islandora/object/auislandora%3A68456/datastream/PDF/view

Denning, D. E. (2010). Terror's web: How the Internet is transforming terrorism. Dans Y. Jewkes et M. Yar (dir.), *Handbook of internet crime* (p.194-213). Cullompton & Portland : Willan publishing.

De Seta, G. (2018). Biaoqing: The circulation of emoticons, emoji, stickers, and custom images on Chinese digital media platforms. *First Monday*, *23*(9).

Dewey, J. (1916). *Essays in Experimental Logic.* Chicago, IL : University of Chicago Press.

Dewey, H. (1929). *The Quest for Certainty : A Study of the Relation of Knowledge and Action.* New York : Minton, Balch & Company.

Dewey, J. (2014). *Reconstruction en philosophie*. Paris : Gallimard.

Dézé, A. (2007). L'image fixe en questions. Retour sur une enquête de réception du discours graphique du Front national. Dans P. Favre, O. Fillieule et F. Jobard, *L'atelier du politiste* (p. 313-330). Paris : La Découverte.

Dézé, A. (2013). Pour une iconographie de la contestation. *Cultures & conflits*, (91/92), 13-29.

Diani, M. (2000). Social movement networks virtual and real. *Information, Communication & Society*, *3*(3), 386-401.

Dias, K. (2003). The ana sanctuary: Women's pro-anorexia narratives in cyberspace. *Journal of International Women's Studies*, *4*(2), 31-45.

Dodge, M., & Kitchin, R. (2005). Code and the transduction of space. *Annals of the Association of American geographers*, *95*(1), 162-180.

Dodge, M., Kitchin, R., & Zook, M. (2009). How does software make space? Exploring some geographical dimensions of pervasive computing and software studies. *Environment and Planning A : Economy and Space, 40*, 1283-1293.

Dodier, N. (1993). Les arènes des habiletés techniques. Dans B. Conein, N. Dodier et L. Thévenot (dir.), *Les objet dans l'action : De la maison au laboratoire* (p. 115-139). Paris : Raisons pratiques.

Dodier, N. (1995). *Les hommes et les machines : la conscience collective dans les sociétés technicisées*. Paris : Editions Métailié.

Dodier, N., & Baszanger, I. (1997). Totalisation et altérité dans l'enquête ethnographique. *Revue française de sociologie, 38*(1), 37-66.

Domenach, J. M. (1973). *La propagande politique*. Paris : PUF.

Donath, J. (1999). Identity and deception in the virtual community. Dans M. A. Smith & P. Kollock (dir.), *Communities in Cyberspace* (p. 29–59). London & New York : Routledge.

Donovan, J. (2019). How memes got weaponized : A short history. *MIT Technology Review*. Repéré à https://www.technologyreview.com/s/614572/political-war-memes-disinformation/

Dourish, P. (2016). Algorithms and their others: Algorithmic culture in context. *Big Data & Society*, *3*(2), https://doi.org/10.1177/2053951716665128.

Downing, J. (2008). Social movement theories and alternative media: An evaluation and critique. *Communication, Culture & Critique*, *1*(1), 40-50.

Drezner, D. W. (2004). The global governance of the Internet: bringing the state back in. *Political Science Quarterly*, *119*(3), 477-498.

Drucker, J. (2013). Performative Materiality and Theoretical Approaches to Interface. *DHQ: Digital Humanities Quarterly*, *7*(1).

Dubey, A., Maaten, L. V. D., Yalniz, Z., Li, Y., & Mahajan, D. (2019). Defense against adversarial images using web-scale nearest-neighbor search. Dans *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (p. 8767-8776). Repéré à https://arxiv.org/abs/1903.01612

Dubbin, R. (2013, 14 novembre). The rise of Twitter bots. *The New Yorker*. Repéré à https://www.newyorker.com/tech/annals-of-technology/the-rise-of-twitter-bots

Dubois, E., & Blank, G. (2018). The echo chamber is overstated: the moderating effect of political interest and diverse media. *Information, Communication & Society*, *21*(5), 729-745.

Ducol, B. (2015). Comment le jihadisme est-il devenu numérique?. *Sécurité et stratégie*, *20*(1), 34-43.

Dutton, W. H., & Peltu, M. (2007). The emerging Internet governance mosaic: connecting the pieces. *Information Polity*, *12*(1-2), 63-81.

Earl, J. S., & Kimport, K. (2010). The diffusion of different types of internet activism: Suggestive patterns in website adoption of innovations. Dans R.K. Givan, K. M. Roberts et S.A. Soule (dir.), *The Diffusion of Social Movements: Actors, Mechanisms, and Political Effects* (p. 125-139). Cambridge : Cambridge University Press.

Earl, J., & Kimport, K. (2011). *Digitally enabled social change: Activism in the internet age*. Cambridge, MA : MIT Press.

El Difraoui, A. (2013). *Al-Qaida par l'image : la prophétie du martyre*. Paris : PUF.

El Difraoui, A. (2016). *Le djihadisme : «Que sais-je ?»*. Paris : PUF.

Edwards, C., & Gribbon, L. (2013). Pathways to violent extremism in the digital era. *The RUSI Journal*, *158*(5), 40-47.

Eisenstein, E. L. & Mansuy, G. (1971). L'avènement de l'imprimerie et la Réforme. Annales. Economies, sociétés, civilisations, *26*(6), 1355-1382.

Elin, L. (2003) "The radicalization of Zeke Spier: how the Internet contributes to civic engagement and new forms of social capital". Dans M. McCaughey et D. Ayers (dir.), *Cyberactivism: Online Activism in Theory and Practice* (p. 97-114), London & New York : Routledge.

Eisinger, P. K. (1973). The conditions of protest behavior in American cities. *American political science review*, *67*(1), 11-28.

Ellul, J. (1977). *Le système technicien*. Paris: Calmann-Lévy

Ermoshina, K., & Musiani, F. (2017). Migrating servers, elusive users: Reconfigurations of the Russian Internet in the post-Snowden era. *Media and Communication*, *5*(1), 42-53.

Ernst, N., Engesser, S., Büchel, F., Blassnig, S., & Esser, F. (2017). Extreme parties and populism: an analysis of Facebook and Twitter across six countries. *Information, Communication & Society*, *20*(9), 1347-1364.

Etzioni, A. Etzioni, O. (1999). Face-to-face and computer-mediated communities, a comparative analysis. *The information society*, *15*(4), 241-248.

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. New York, NY : St. Martin's Press.

Evolvi, G. (2019). # Islamexit: inter-group antagonism on Twitter. *Information, Communication & Society*, *22*(3), 386-401.

Eysenbach, G., & Till, J. E. (2001). Ethical issues in qualitative research on internet communities. *Bmj*, *323*(7321), 1103-1105.

Farrell, H. (2012). The consequences of the internet for politics. *Annual review of political science*, *15,* 35-52.

Farwell, J. P. (2014). The media strategy of ISIS. *Survival*, *56*(6), 49-55.

Feeley, M. M., & Simon, J. (1992). The new penology: Notes on the emerging strategy of corrections and its implications. *Criminology*, *30*(4), 449-474.

Feenberg, A. (2004). *(Re) penser la technique : vers une technologie démocratique*. Paris : La Découverte.

Feenberg, A. (2014). *Pour une théorie critique de la technique*. Montréal : Lux.

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM*, *59*(7), 96-104.

Ferrara, E., Wang, W. Q., Varol, O., Flammini, A., & Galstyan, A. (2016). Predicting online extremism, content adopters, and interaction reciprocity. Dans *International conference on social informatics* (p. 22-39). Repéré à https://arxiv.org/abs/1605.00659

Fillieule, O. et Péchu, C. (1993). Lutter ensemble. Les théories de l'action collective. Paris : L'Harmattan.

Fischer, P., Fischer, J. K., Weisweiler, S., & Frey, D. (2010). Terrorism as collective communication: The collective communication model of terrorism (CCMT). *Social and Personality Psychology Compass*, *4*(9), 692-703.

Flichy, P. (2008a). Internet et le débat démocratique. *Réseaux*, (4), 159-185

Flichy, P. (2008b). Technique, usage et représentations. *Réseaux*, (2), 147-174.

Fligstein, N. (2001). Le mythe du marché. *Actes de la recherche en sciences sociales*, (4), 3-12.

Forelle, M., Howard, P., Monroy-Hernández, A., & Savage, S. (2015). Political bots and the manipulation of public opinion in Venezuela. *arXiv preprint arXiv:1507.07109*. Repéré à https://arxiv.org/abs/1507.07109.

Foster, H. (1988). Préface. Dans H. Foster (dir.), *Vision and visuality* (p.ix-xiv). Seattle : Bay press.

Foucault, M. (1975). *Surveiller et punir*. Paris : Gallimard.

Foucault, M. (1978). *Sécurité, territoire, population. Cours au Collège de France, 1977-1978*. Paris : Gallimard.

Foucualt, M. (1994). *Dits et écrits, II : 1976-1988*. Paris: Gallimard.

Foust, C. R., & Hoyt, K. D. (2018). Social movement 2.0: Integrating and assessing scholarship on social media and movement. *Review of Communication*, *18*(1), 37-55.

Fuchs, C. (2014). Social media and the public sphere. *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, *12*(1), 57-101.

Fuller, M. (2008). *Software Studies : A Lexicon.* Cambridge, MA :MIT Press

Fuller, M., & Goffey, A. (2012). *Evil media*. Cambridge, MA : MIT Press.

Fung, A. & Shkabatur, J. (2015). Viral engagement : Fast, cheap, and broad, but good for democracy ? Dans D. Allen et J.S. Light (dir.), *From voice to influence: Understanding citizenship in a digital age* (p. 155-177). Chicago, IL : University of Chicago Press.

Galloway, A. R. (2004). *Protocol: How control exists after decentralization*. Cambridge, MA : MIT Press.

Galloway, A. R. (2006). *Gaming: Essays on algorithmic culture*. Minneapolis, MN : University of Minnesota Press.

Galloway, A. R. (2012). *The interface effect*. Cambridge : Polity.

Gamson, W. A. (1975). *The strategy of social protest*. Homewood, IL : The Dorsey Press.

Gamson, W. A., Fireman, B., & Rytina, S. (1982). *Encounters with unjust authority*. Homewood, IL : The Dorsey Press..

Gamson, W. A (1992). *Talking politics*. Cambridge : Cambridge university press.

Gamson, W.A. (1990) *The Strategy of Social Protest*. Belmont, CA: Wadsworth.

Gamson, W. A., & Wolfsfeld, G. (1993). Movements and media as interacting systems. *The Annals of the American Academy of Political and Social Science*, *528*(1), 114-125.

Ganesh, B., & Bright, J. (2020). Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation. *Policy & Internet*, *12*(1), 6-19.

Garrett, K. R. (2006). Protest in an information society: A review of literature on social movements and new ICTs. *Information, communication & society*, *9*(02), 202-224.

Gates, S., & Podder, S. (2015). Social media, recruitment, allegiance and the Islamic State. *Perspectives on Terrorism*, *9*(4).

Gates, K. (2019). Policing as Digital Platform. *Surveillance & Society*, *17*(1/2), 63-68.

Gattinara, P.C., & Bouron, S. (2019). Extreme-right communication in Italy and France: political culture and media practices in CasaPound Italia and Les Identitaires. *Information, Communication & Society*, 1-15.

Geertz, C. (1998). La description dense. Vers une théorie interprétative de la culture. *Enquête. Archives de la revue Enquête*, (6), 73-105.

Gehl, R. W. (2014). *Reverse engineering social media: Software, culture, and political economy in new media capitalism*. Philadelphia, PA : Temple University Press.

George, E. (2002). Dynamiques d'échanges publics sur Internet. Dans F. Jauréguiberry et S. Proulx (dir.), *Internet, nouvel espace citoyen ?* (pp.49-80). Paris : L'harmattan.

Gerbaudo, P. (2012). *Tweets and the Streets*. London: Pluto Press.

Gergorin, JL. & Isaac-Dognin, L. (2018). *Cyber, la guerre permanente*. Pars : CERF.

Gerstenfeld, P. B., Grant, D. R., & Chiang, C. P. (2003). Hate online: A content analysis of extremist Internet sites. *Analyses of social issues and public policy*, *3*(1), 29-44.

Ghajar-Khosravi, S., Kwantes, P., Derbentseva, N., & Huey, L. (2016). Quantifying salient concepts discussed in social media content: An analysis of tweets posted by ISIS fangirls. *Journal of Terrorism Research*, *7*(2), 79-90.

Ghonim, W. (2012). *Revolution 2.0: The power of the people is greater than the people in power: A memoir*. Boston, MA : Houghton Mifflin harcourt.

Gibson, J. J. (1977). The theory of affordances. Dans J. J. Gieseking, W. Mangold, C. Katz, S. Low et S. Saegert (dir.), *The People, Place and Space Reader* (p.56-60). London & New York : Routledge.

Gill, P., Corner, E., Thornton, A., & Conway, M. (2015). What are the roles of the Internet in terrorism? Measuring online behaviours of convicted UK terrorists. *VOX-Pol Network of Excellence*. Répéré à : http://www.voxpol.eu/what-are-the-roles-of-the-internet-in-terrorism/

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the Internet by the numbers: Quantifying behaviors, patterns, and processes. *Criminology & Public Policy*, *16*(1), 99-117.

Gille, B. (1978). *Histoire des techniques.* Paris: Gallimard.

Gillespie, T. (2010). The politics of "platforms". *New media & society*, *12*(3), 347-364.

Gillespie, T. (2014). The Relevance of Algorithms. Dans T. Gillespie, P. Boczkowski et K. Foot (dir.), *Media Technologies : Essays on Communication, Materiality, and Society,* (p. 167-195). Cambridge, MA: MIT Press.

Gillespie, T. (2016). Algorithms. Dans B. Peters (dir.), *Digital keywords: a vocabulary of information society and culture*. Princeton, NJ : Princeton University Press.

Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. New Haven, CT : Yale University Press.

Gimmler, A. (2001). Deliberative democracy, the public sphere and the internet. *Philosophy & Social Criticism*, *27*(4), 21-39.

Gitelman, L. (dir.). (2013). *Raw data is an oxymoron*. Cambridge, MA : MIT Press.

Gitelman, L., & Jackson, V. (2013). *Introduction*. Dans L. Gitelman, *"Raw Data" is an Oxymoron* (p. 1-15). Cambridge, MA : MIT press.

Gitlin, T. (1977). Spotlights and shadows: television and the culture of politics. *College English*, *38*(8), 789-801.

Gitlin, T. (1980) *The whole world is watching: Mass media in the making and unmaking of the new left*. Berkeley, CA: University of California Press.

Gladwell, M. (2010, 27 septembre). Small Change : Why the Revolution Will Not Be Tweeted. *New Yorker*. Repéré à https://www.newyorker.com/magazine/2010/10/04/small-change-malcolm-gladwell

Glasman, F. (2014). Vie locale et concurrence de projets politiques dans les territoires sous contrôle de l'opposition, des djihadistes et des Kurdes en Syrie. *Ministrère de la Défense, France.* Repéré à https://www.academia.edu/10032604/Vie_locale_et_concurrence_de_projets_politiques_dans_les_territoires_sous_contrôle_de_lopposition_des_djihadistes_et_des_Kurdes_en_Syrie

Goddard, M. (2011). Towards an Archaeology of Media Ecologies:"Media Ecology. Political Subjectivation and Free Radios". *Fibreculture,* 17, 6-17.

Goldsmith J. & Wu T. (2006) *Who Controls the Internet? Illusions of a Borderless World*. Oxford : Oxford University Press.

Gomm, R., Hammersley, M., & Foster, P. (dir.) (2000). *Case study method: Key issues, key texts*. Thousand Oaks, CA : SAGE.

Gonzales, A. (2016). The contemporary US digital divide: from initial access to technology maintenance. *Information, Communication & Society*, *19*(2), 234-248.

Goodwin, J., Jasper, J. M., & Polletta, F. (2004). Emotional dimensions of social movements. *The Blackwell companion to social movements*, 413-432.

Goodwin, J., Jasper, J. M., & Polletta, F. (2001). Why emotions matter. Dans H. Goodwin, J. M. Jasper et F. Polletta (dir.), *Introduction to Passionate Politics : Emotions and Social Movements* (p. 1-24). Chicago, IL : University of Chicago Press.

Graham, G. (1999). *The Internet: a philosophical inquiry*. London & New York : Routledge.

Graham, M., Hjorth, I., & Lehdonvirta, V. (2017). Digital labour and development: impacts of global digital labour platforms and the gig economy on worker livelihoods. *Transfer: European Review of Labour and Research*, *23*(2), 135-162.

Gras, S. E. (2015). Éthique computationnelle et matérialisme numérique : l'apport des Software Studies. *Critique*, (8), 667-679.

Granjon, F. (2003). Les militants-internautes. Passeurs, filtreurs et interprètes. *Communication. Information médias théories pratiques*, *22*(1), 11-32.

Granjon, F. (2009). Média. Dans O. Fillieule, L. Mathieu et C. Péchu (dir.), *Dictionnaire des mouvements sociaux* (p. 341-348). Paris : Presses de Sciences Po.

Greenberg, J. (2015, 21 novembre). Why Facebook and Twitter can't just wipe out ISIS online. *Wired.* Repéré à https://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media/

Greenleaf, G. (1998). An endnote on Regulating Cyberspace : Architecture vs Law.*University of New South Wales Law Journal,* (21), 593-622.

Grimmelmann, J. (2015). The virtues of moderation. *Yale JL & Tech.*, *17*, 42-110.

Grint, K., & Woolgar, S. (1995). On some failures of nerve in constructivist and feminist analyses of technology. *Science, Technology, & Human Values*, *20*(3), 286-310.

Groves, J. M. (1997). *Hearts and minds: The controversy over laboratory animals*. Philadelphia, PA : Temple University Press.

Gurak, L.J. (1997) *Persuasion and Privacy in Cyberspace: The Online Protests over Lotus Marketplace and the Clipper Chip*. New Haven, CT : Yale University Press.

Hall, S. (1973). The determinations of news photographs. Dans S. Cohen & J. Young (dir.), *The manufacture of news* (p. 176-191). Thousand Oaks, CA : SAGE.

Hall, S. (1994). Codage/décodage (traduit par M. Albaret et M. C. Gamberini). *Réseaux. Communication-Technologie-Société*, *12*(68), 27-39.

Hamburger, J. F. (1997). *Nuns as artists: the visual culture of a medieval convent*. California : University of California Press.

Hamel, J. (1997). *Étude de cas et sciences sociales*. Paris : Harmattan.

Hamel, J. (1998). Défense et illustration de la méthode des études de cas en sociologie et en anthropologie. Quelques notes et rappels. *Cahiers internationaux de sociologie*, 121-138.

Hammersley, M., & Atkinson, P. (2007). *Ethnography : Principles in practice*. London and New York: Routledge.

Hammersley, M., & Gom, R. (2000). Introduction. Dans R. Gomm, M. Hammersely et P. Foster (dir.), *Case study method : Key issues, key texts* (p. 234-258). Thousand Oaks, CA : SAGE.

Haraway, D. (1991). *Simians, cyborgs, and women: The reinvention of nature*. London & New York : Routledge.

Hargittai, E. (2002). Second-level digital divide: Differences in people's online skills. *First monday*, *7*(4).

Harling, P. (2014, septembre). État islamique, un monstre providentiel. *Le monde diplomatique*. Repéré à https://www.monde-diplomatique.fr/2014/09/HARLING/50787

Harlow, S. (2012). Social media and social movements: Facebook and an online Guatemalan justice movement that moved offline. *New Media & Society*, *14*(2), 225-243.

Hauben, M., & Hauben, R. (1998). Netizens: On the history and impact of Usenet and the Internet. *First Monday*, *3*(7).

Hayles (2015). *Parole, écriture, code* (traduit par S. Vanderhaeghe). Paris : Les presses du réel.

Hecker, M. (2015). Web social et djihadisme : Du diagnostic aux remèdes. *Ifri Centre des études de sécurité focus stratégique n° 57*. Repéré à https://www.ifri.org/fr/publications/enotes/focus-strategique/web-social-djihadisme-diagnostic-aux-remedes.

Hecker, M. (2018). 137 nuances de terrorisme. Les djihadistes de France face à la justice. *Ifri Centre des études de sécurité focus stratégique n° 79.* Repéré à https://www.ifri.org/fr/publications/etudes-de-lifri/focus-strategique/137-nuances-de-terrorisme-djihadistes-de-france-face

Hegelich, S., & Janetzko, D. (2016). Are Social Bots on Twitter Political Actors? Empirical Evidence from a Ukrainian Social Botnet. Dans *ICWSM* (p. 579-582). Repéré à https://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13015/12793

Hegghammer, T. (2009). The ideological hybridization of Jihadi groups. *Current Trends in Islamist Ideology*, *9*(1), 26-45.

Hegghammer, T. (2016). Violence politique en Arabie Saoudite : Grandeur et décadence d'« Al-Qaïda dans la péninsule arabique ». Dans B. Rougier (dir), *Qu'est-ce que le salafisme* (p.105-123). Paris : PUF.

Heinich, N. (2012). *De la visibilité. Excellence et singularité en régime médiatique*. Paris : Gallimard.

Helberger, N. (2015). Public service media| merely facilitating or actively stimulating diverse media choices? public service media at the crossroad. *International Journal of Communication*, *9*, 17.

Helberger, N., Karppinen, K., & D'acunto, L. (2018). Exposure diversity as a design principle for recommender systems. *Information, Communication & Society*, *21*(2), 191-207.

Helmond, A. (2015). The platformization of the web: Making web data platform ready. *Social Media+ Society*, *1*(2), https://doi.org/10.1177/2056305115603080.

Hénin, N. (2015). *Jihad Academy*. Paris : Fayard.

Hill, K. A., & Hughes, J. E. (1998). *Cyberpolitics: Citizen activism in the age of the Internet*. Lanham, MD : Rowman & Littlefield Publishers.

Hillis, K., Petit, M., & Jarrett, K. (2013). *Google and the Culture of Search*. London & New York : Routledge.

Hine, C. (2000). *Virtual ethnography*. Thousand Oaks, CA : SAGE.

Hine, C. (2008). Virtual ethnography: Modes, varieties, affordances. Dans G. Blank, N. Fielding et L. M. Raymond (dir.), *The SAGE handbook of online research methods* (p. 257-270). Thousand Oaks, CA : SAGE.

Hine, C. (2009). Question one: how can Internet researchers define the boundaries of their project. Dans A. Markham et N. Baym (dir.), *Internet inquiry : Conversations about method* (p.1-20). Thousand Oaks, CA : SAGE.

Hoar, P. and W. Hope (2002) "The Internet, the Public Sphere and the 'Digital Divide' in New Zealand", *Journal of International Communication* 8(2): 64–88.

Hogan, M. (2015). Facebook data storage centers as the archive's underbelly. *Television & New Media*, *16*(1), 3-18.

Hoffman, B. (1999). *La mécanique terroriste*. Paris : Calman-Lévy.

Honneth, A. (2005). Invisibilité : sur l'épistémologie de la «reconnaissance». *Réseaux*, *129*(1), 39-57.

Hooley, T, Wellens, J, Marriott, J (2011) *What Is Online Research: Using the Internet for Social Science Research.* New York, NY : Bloomsbury Academic.

Horrigan, J.B. (2001) Online Communities: Networks that Nurture Long-distance Relationships and Local Ties. *Pew Internet & American Life Project*. Repéré à http://www.pewinternet.org/pdfs/PIP_Communities_ Report.pdf

Horrigan, J.B, Garrett, K., & Resnick, K. (2004) *The Internet and Democratic Debate*. Washington, DC: Pew Internet & American Life Project.

Howard, P. N., & Kollanyi, B. (2016). Bots,# StrongerIn, and# Brexit: computational propaganda during the UK-EU referendum. *Working Paper 2016.1. Oxford, UK: Project on Computational Propaganda*. Repéré à www.politicalbots.org. http://dx.doi.org/10.2139/ssrn.2798311.

Howard, P., Kollanyi, B., & Woolley, S. C. (2016). Bots and Automation over Twitter during the Second US Presidential Debate. *Data Memo 2016.2. Oxford, UK: Project on Computational Propaganda*. Repéré à http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2016/11/Data-Memo-US-Election.pdf.

Howes, D. (dir.) (1991). *The Varieties of Sensual Experience : A sourcebook in the Anthropology of the Senses.* Toronto : University of Toronto Press.

Hsu, C. L., & Park, H. W. (2011). Sociology of hyperlink networks of Web 1.0, Web 2.0, and Twitter: A case study of South Korea. *Social science computer review*, *29*(3), 354-368.

Hubac-Occhipinti, O. (2015). Les terroristes anarchistes du XIXème Siècle. Dans G. Chaliand & A. Blin (dir.), *Histoire du terrorisme : de l'antiquité à Al Qaida* (p.151-175). Villeneuve-d'Ascq : Fayard.

Hubert, M. (2014). *Partager des expériences de laboratoire : La recherche à l'épreuve des réorganisations.* Paris : Éditions des archives contemporaines.

Huey, L. (2015). This is Not Your Mother's Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming. *Journal of Terrorism Research*, *6*(2), 1-16.

Huey, L., Inch, R., & Peladeau, H. (2019). "@ me if you need shoutout": Exploring Women's Roles in Islamic State Twitter Networks. *Studies in Conflict & Terrorism*, *42*(5), 445-463.

Hughes, T.P. (1983). *Networks of Power. Electrification in Western Society 1880-1930*. Baltimore, MD : The John Hopkins University Press.

Hughes, T. P. (1987). The evolution of large technological systems. Dans W. E. Bijker, T. P. Hughes et T. Pinch (dir.), *The social construction of technological systems: New directions in the sociology and history of technology* (p. 51-82). Cambridge, MA : MIT Press.

Huntington, H. E. (2016). Pepper spray cop and the American dream: Using synecdoche and metaphor to unlock Internet memes' visual political rhetoric. *Communication Studies*, *67*(1), 77-93.

Hutchby, I. (2001). Technologies, texts and affordances. *Sociology*, *35*(2), 441-456.

Hwang, T., Pearce, I., & Nanis, M. (2012). Socialbots: Voices from the fronts. *Interactions*, *19*(2), 38-45.

Illari, P., & Russo, F. (2014). *Causality: Philosophical theory meets scientific practice*. Oxford : Oxford University Press.

Ingram, H. J. (2016). An analysis of Islamic State's Dabiq magazine. *Australian Journal of Political Science*, *51*(3), 458-477.

Introna, L. D. (2007). Maintaining the reversibility of foldings: Making the ethics (politics) of information technology visible. *Ethics and Information Technology*, *9*(1), 11-25.

Jackson, M.H. (1996). The meaning of "communication technology": The technology–context scheme. Dans B. Burleson (dir.), *Communication Yearbook* (vol. 19) (p. 229-267). Thousand Oaks, CA : SAGE.

Jasper, J. (1997). The Art of Moral Protest. Culture, Biography and Creativity in Social Movements. Chicago, IL : University of Chicago Press.

Jay, M. (1993). *Downcast eyes: The denigration of vision in twentieth-century French thought*. California, CA : University of California Press.

Jay, M., & Brennan, T. (dir.). (1996). *Vision in context: historical and contemporary perspectives on sight*. London & New York : Routledge.

JDN rédaction (2019, 29 novembre). Nombre d'utilisateurs de Twitter dans le monde. Journal du net. Repéré à : https://www.journaldunet.com/ebusiness/le-net/1159246-nombre-d-utilisateurs-de-twitter-dans-le-monde/.

Jeanneret, Y. (2011). Complexité de la notion de trace. De la traque au tracé. Dans Galinon-Melenec (dir.), *L'Homme trace. Perspectives anthropologiques des traces contemporaines* (p. 59-86). Paris : CNRS Éditions.

Jenkins, H. (2006). *Convegence Culture : Where Old and New Media Collide*. New York, NY : University Press.

Johnson, D. R., & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, 1367-1402.

Jones, S (1998) *Doing Internet Research: Critical Issues and Methods for Examining the Net*. Thousand Oaks, CA : SAGE.

Jouët, J., & Le Caroff, C. (2013). L'observation ethnographique en ligne. Dans C. Barats (dir.), *Manuel d'analyse web en Sciences Humaines et Sociales* (p. 147-165). Malakoff : Armand Colin.

Jurgenson, N. (2012). When atoms meet bits: Social media, the mobile web and augmented revolution. *Future Internet*, *4*(1), 83-91.

Jurgenson, N. (2014, 9 octobre). View From Nowhere. *The New Inquiry*. https://thenewinquiry.com/view-from-nowhere/

Juris, J. S. (2005). The new digital media and activist networking within anti–corporate globalization movements. *The Annals of the American Academy of Political and Social Science*, *597*(1), 189-208.

Juris, J. S. (2012). Reflections on# Occupy Everywhere: Social media, public space, and emerging logics of aggregation. *American Ethnologist*, *39*(2), 259-279.

Kahn, R., & Kellner, D. (2004). New media and internet activism: from the 'Battle of Seattle'to blogging. *New media & society*, *6*(1), 87-95.

Kahn, R. and Kellner, D., (2008). Technopolitics, blogs, and emergent media ecologies: A critical/reconstructive approach. Dans B. Hawk, D.M. Riedler et O. Oviedo (dir.), *Small tech: the culture of digital tools* (p. 22-37). Minnesota, MN : University of Minnesota Press.

Kallinikos, J. (2012). Form, function, and matter: Crossing the border of materiality. Dans P. M. Leonardi, B. A. Nardi & J. Kallinikos (dir.), *Materiality and organizing: Social interaction in a technological world* (p. 67-87). Oxford : Oxford University Press.

Kantrowitz, A. (2018, 19 janvier). More Than 50,000 Russia-Linked Bots Tweeted About The Election During The 2016 Campaign. *BuzzFeed*. Repéré à https://www.buzzfeed.com/ alexkantrowitz/more-than-50000-russia-linked-bots-tweeted-about-the?bftwnews&utm_ term=.crZelJnnlZ#.qgOGAKrrA8.

Kendall, L. (2002). *Hanging out in the virtual pub: Masculinities and relationships online*. Berkeley, CA: University of California Press.

Kinsley, S. (2014). The matter of "virtual'geographies''. *Progress in Human Geography*, *38*(3), 364-384.

Kirschenbaum, M. G. (2003). Virtuality and VRML: Software studies after Manovich. *Electronic Book Review* [En ligne]. Repéré à https://electronicbookreview.com/essay/virtuality-and-vrml-software-studies-after-manovich/

Kirschenbaum, M. G. (2008). *Mechanisms: New media and the forensic imagination*. Cambridge, MA : MIT Press.

Kitchin, R. (2014a). Big Data, new epistemologies and paradigm shifts. *Big data & society*, *1*(1), https://doi.org/10.1177/2053951714528481.

Kitchin, R. (2014b). *The data revolution: Big data, open data, data infrastructures and their consequences*. Thousand Oaks, CA : SAGE.

Kitchin, R. (2017). Thinking critically about and researching algorithms. *Information, Communication & Society*, *20*(1), 14-29.

Kittler, F. (1995). There is no software. *Ctheory* [en ligne]. Repéré à http://www.ctheory.net/articles.aspx?id=74

Klandermans, B., & Oegema, D. (1987). Potentials, networks, motivations, and barriers: Steps towards participation in social movements. *American sociological review*, *52*(4) 519-531.

Klausen, J. (2015). Tweeting the Jihad: Social media networks of Western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism*, *38*(1), 1-22.

Klein, H. (2002). ICANN et la gouvernance d'internet. *Les cahiers du numérique*, *3*(2), 91-128.

Kleinman, S.S. (2004). Researching OURNET: A Case Study of a Multiple Methods Approach. Dans J. D. Mark, C. S. Ling & J. G. Hall (dir.), *Online Social Research: Methods, Issues, and Ethics* (p. 47-62). New York, NY : Peter Lang.

Kligler-Vilenchik, N., & Thorson, K. (2016). Good citizenship as a frame contest: Kony2012, memes, and critiques of the networked citizen. *New Media & Society*, *18*(9), 1993-2011.

Kline, S. J., & Rosenberg, N. (2010). An overview of innovation. Dans K. F. Hew et W. S. Cheung (dir.), *Studies On Science And The Innovation Process: Selected Works of Nathan Rosenberg* (p. 173-203). Chicago : Academy of Engineering Press.

Koerner, B. (2016, avril). Why ISIS Is Winning the Social Media War. *Wired*. Repéré à http://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/

Kowalski, R. (1979). Algorithm= logic+ control. *Communications of the ACM*, *22*(7), 424-436.

Kozinets, R. V. (2010). *Netnography : Doing Ethnographic Research Online*. Thousand Oaks, CA : SAGE.

Krämer, B. (2017). Populist online practices: the function of the Internet in right-wing populism. *Information, Communication & Society*, *20*(9), 1293-1309.

Kraidy, M. M. (2017). The projectilic image: Islamic State's digital visual warfare and global networked affect. *Media, Culture & Society*, *39*(8), 1194-1209.

Kushner, S. (2013). The freelance translation machine: Algorithmic culture and the invisible industry. *New Media & Society*, *15*(8), 1241-1258.

Kwok Choon, M.-J., Proulx, S. (2011). Luttes pour la reconnaissance des groupes associatifs : l'usage de Facebook par deux ONG de l'île Maurice. Dans S. Proulx, M. Millette & L. Heaton (dir.), *Médias sociaux : enjeux pour la communication* (p.81-103). Québec : Presses de l'Université du Québec.

Lacey, C. (1970). *Hightown Grammar*. Manchester : Manchester University Press.

Lacey, C. (1976). "Problems of sociological fieldwork a review of the methodology of Hightown Grammar", Dans M. Shipman (dir.). *The Organization and Impact of Social Research*. London : Routledge & Kegan Paul. London & New York : Routledge.

Langley, P., & Leyshon, A. (2017). Platform capitalism: the intermediation and capitalisation of digital economic circulation. *Finance and society.*, *3*(1), 11-31.

Langlois, G., McKelvey, F., Elmer, G., & Werbin, K. (2009a). Mapping commercial Web 2.0 worlds: Towards a new critical ontogenesis. *Fibreculture*, 14. Repéré à http://fourteen.fibreculturejournal.org/fcj-095-mapping-commercial-web-2-0-worlds-towards-a-new-critical-ontogenesis09.

Langlois, G., Elmer, G., McKelvey, F., & Devereaux, Z. (2009b). Networked publics: The double articulation of code and politics on Facebook. *Canadian Journal of Communication*, *34*(3), 415-434.

Langlois, G., & Elmer, G. (2013). The research politics of social media platforms. *Culture machine*, *14*, 1-17.

Lash, S. (2007). Power after hegemony: Cultural studies in mutation?. *Theory, culture & society*, *24*(3), 55-78.

Latour, B. (1984). *Pasteur : guerre et paix des microbes ; suivi de Irréductions*. Paris : La découverte.

Latour, B. (1989). *La science en action.* Paris : La Découverte.

Latour, B. (1991a). Technology is Society Made Durable. Dans J. Law (dir.), *A Sociology of Monsters* (103-131). London & New York : Routledge..

Latour, B. (1991b). *Nous n'avons jamais été modernes : Essai d'anthropologie symétrique*. Paris : La Découverte.

Latour, B. (1993). *La clef de Berlin ; et autres leçons d'un amateur de sciences*. Paris : La Découverte.

Latour, B. (1994). Une sociologie sans objet ? Note théorique sur l'interobjectivité. *Sociologie du travail*, *36*(36), 587-607.

Latour, B. (2000). When things strike back: a possible contribution of "science studies" to the social sciences. *The British journal of sociology*, *51*(1), 107-123.

Latour, B. (2001). *L'espoir de Pandore. Pour une version réaliste de l'activité scientifique*. Paris : La Découverte.

Latour, B. (2006a). *Ré-assembler le social, introduction à une théorie de l'acteur*. Paris : La Découverte.

Latour, B. (2006b). Flot et défaut des images : de l'iconoclasme et l'iconoclash. Dans L. Gervereau (dir.), *Dictionnaire des images* (p. 122-200). Paris : Édition Nouveau Monde.

Latour, B. (2007). Paris, ville invisible : le plasma. Dans C. Macel et V. Guillaume (dir.), *Airs de Paris – 30 ans du Centre Pompidou* (p. 260-263). Paris : Éditions de la Bibliothèque publique d'information.

Latour, B. (2012). *Enquête sur les modes d'existence. Une anthropologie des Modernes*. Paris : La Découverte.

Latour, B., Mauguin, P., & Teil, G. (1991). Une méthode nouvelle de suivi socio-technique des innovations : le graphe socio-technique. Dans Dominique V. (dir.), *Gestion de la recherche : nouveaux problèmes, nouveaux défis* (p. 419-477). Louvain-la-Neuve : Editions de Boeck

Latour, B., & Woolgar, S. (1996). *La vie de laboratoire : la production des faits scientifiques*. Paris : La Découverte.

Latzko-Toth, G. (2009). L'étude de cas en sociologie des sciences et des techniques. *Notes de recherche du CIRST*. Repéré à www.cirst.uqam.ca/Portals/0/docs/note_rech/2009-03.pdf

Law, J. (1987). Technology and heterogeneous engineering: The case of Portuguese expansion. Dans W. E. Bijker, T. P. Hughes et T. Pinch (dir.), *The social construction of technological systems: New directions in the sociology and history of technology* (p. 105-128). Cambridge, MA : MIT Press.

Law, J. (1992). Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity. *Systems practice*, *5*(4), 379-393.

Law, J. (1994). *Organizing modernity*. Oxford: Blackwell.

Law, J. (1999). After ANT : complexity, naming and topology. Dans J. Law et J. Hassard (dir.), *Actor Network Theory and After* (p. 1-15). Oxford and Malden : Blackwell Publishers.

Law, J. (2004). *After method: Mess in social science research*. London & New York : Routledge.

Law, J. (2009). Actor network theory and material semiotics. Dans B. S. Turner (dir.), *The new Blackwell companion to social theory* (p. 141-158). Chichester, UK : John & Sons.

Law, J., & Callon, M. (1992). The life and death of an aircraft: a network analysis of technical change. Dans W. Bijker et J. Law (dir.), *Shaping Technology/Building Society* (p. 21-52). Cambridge, MA : MIT Press.

Law, J. & Hassard, J. (1999). *Actor Network Theory and After*. Oxford and Malden : Blackwell Publishers.

Leadbeater, C. (2008). *We-Think*. London : Profile Books.

Lemieux, C. (2018). *La sociologie pragmatique*. Paris : La Découverte.

Leizerov, S. (2000). Privacy advocacy groups versus Intel: A case study of how social movements are tactically using the Internet to fight corporations. *Social science computer review*, *18*(4), 461-483.

Leonardi, P. M. (2007). Activating the informational capabilities of information technology for organizational change. *Organization science*, *18*(5), 813-831.

Leonardi, P. M. (2010). Digital materiality? How artifacts without matter, matter. *First monday*, *15*(6).

Leonardi, P. M. (2012). Materiality, sociomateriality, and socio-technical systems: What do these terms mean? How are they different? Do we need them. Dans P. M. Leonardi, B. A. Nardi & J. Kallinikos (dir.), *Materiality and organizing: Social interaction in a technological world* (p. 25-49). Oxford : Oxford University Press.

Leonardi, P. M., & Barley, S. R. (2008). Materiality and change: Challenges to building better theory about technology and organizing. *Information and organization*, *18*(3), 159-176.

Lessig, L. (2000). Code is law: On liberty in cyberspace. *Harvard Magazine*. Repéré à https://harvardmagazine.com/2000/01/code-is-law-html.

Lessig, L. (2006). *Code version 2.0.* New York : Basic Books.

Lévi-Strauss, C. (1962). *La pensée sauvage*. Paris : Plon.

Levy, S. (2014). *L'Ethique des hackers* (traduit par G. Tordjman). Paris : Globe.

Licoppe, C. (2010). Michel Callon et le « tournant performatif » de la théorie de l'acteur-réseau. Dans M. Akrich, Y. Barth, F. Muniesa et P. Mustar (dir.), *Débordements* (p. 291-298). Paris : Presses des Mines.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New media & society*, *10*(3), 393-411.

Loader, B. D., & Mercea, D. (2011). Networking democracy? Social media innovations and participatory politics. *Information, Communication & Society*, *14*(6), 757-769.

Lokot, T., & Diakopoulos, N. (2016). News bots: Automating news and information dissemination on Twitter. *Digital Journalism*, *4*(6), 682-699.

Lorenzo-Dus, N., & Macdonald, S. (2018). Othering the West in the online Jihadist propaganda magazines Inspire and Dabiq. *Journal of Language Aggression and Conflict*, *6*(1), 79-106.

Loveluck, B. (2016). Les formes du pouvoir sur Internet. Dans J.F. Dortier (dir.), *La Communication : des relations interpersonnelles aux réseaux sociaux, Auxerre, Sciences humaines éditions* (p. 324-335). Auxerre : Éditions Sciences humaines.

Luizard, P.-J. (2017). *Le piège Daech : L'État islamique ou le retour de l'Histoire.* Paris : La Découvete.

Mabi, C. (2016). Analyser les dispositifs participatifs par leur design. Dans C. Barats (dir.), *Manuel d'analyse du Web* (p.33-37). Malakoff : Armand Colin.

Macé, E. (2006). Mouvements et contre-mouvements culturels dans la sphère publique et les médiacultures. Dans E. Maigret et E. Macé (dir.), *Penser les médiacultures. Nouvelles pratiques et nouvelles approches de la représentation du monde* (p.1-21). Paris : Armand Colin.

Mac Carthy, J.D. & Zald, M.N. (1973). *The Trend of Social Movements in America : Professionalization and Resource Mobolization*. Morristown, NJ : General Learning Press.

McCarthy, J. D., & Zald, M. N. (1977). Resource mobilization and social movements: A partial theory. *American journal of sociology*, *82*(6), 1212-1241.

Mackenzie, A. (2003a). Transduction: invention, innovation and collective life. *Institute for Cultural Research, Lancaster University*. Repéré à *http://www. lancs. ac. uk/staff/mackenza/papers/transduction. pdf*

Mackenzie, A. (2003). The problem of computer code: Leviathan or common power. *Institute for Cultural Research, Lancaster University*. Repéré à https://www.lancaster.ac.uk/staff/mackenza/papers/code-leviathan.pdf

Mackenzie, A. (2006). *Cutting code: Software and sociality*. Berne : Peter Lang.

MacKinnon, R. (2012). *Consent of the Networked: The worldwide struggle for internet freedom.* New York, NY : Basic Books.

Maher, S. (2016). *Salafi-Jihadism: The history of an idea*. Oxford : Oxford University Press.

Mahlouly, D. & Winter, C. (2018). A tale of two caliphates : Comparing in the Islamic State's internal and external messaging priorities. *VOX-Pol Network of Excellence*. Répéré à : https://eprints.soas.ac.uk/31122/1/A-Tale-of-Two-Caliphates-Mahlouly-and-Winter.pdf

Mann, C., & Stewart, F. (2000) *Internet Communication and Qualitative Research: A Handbook for Researching Online*. Thousand Oaks, CA : SAGE.

Mannell, K. (2017). Technology Resistance and de Certeau: Deceptive texting as a Tactic of Everyday Life. *PLATFORM: Journal of Media & Communication*, *8*(1).

Manovich, L. (2010). *Le langage des nouveaux médias*. Dijon : Les Presses du réel.

Manovich, L. (2011). *Trending: The promises and challenges of big social data*. Repéré à http://www. manovich. net/DOCS. Manovich_trending_paper. pdf.

Marcus, G. E. (1995). Ethnography in/of the world system: The emergence of multi-sited ethnography. *Annual review of anthropology*, *24*(1), 95-117.

Marcuse, H. (1968). *L'homme unidimensionnel*. Paris : Éditions de minuit.

Marichal, J. (2013). Political Facebook groups: Micro-activism and the digital front stage. *First Monday*, *18*(12).

Markham, A. (2006). Method as ethic, ethic as method. *Journal of Information Ethics*, 15(2), 37–54.

Markham, A. (2011). Internet researcher. Dans D. Silverman (dir.), *Qualitative Research : Theory, Method, and Practices* (3e éd.) (p. 111-128). London : SAGE.

Markham, A., Buchanan, E. et al. (2012). Ethical decision-making and internet research: Version 2.0. recommendations from the AoIR ethics working committee. *AoIR*. Repéré à aoir. org/reports/ethics2.pdf.

Marres, N. (2017). *Digital sociology: The reinvention of social research*. Cambridge : John Wiley & Sons.

Martin, J. L. (1985). The media's role in international terrorism. *Terrorism: An Interna-tional Journal, 8,* 127–146.

Marwick, A. E. (2013). *Status update: Celebrity, publicity, and branding in the social media age*. New Haven, CT : Yale University Press.

Marwick, A. E., & boyd, D. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New media & society*, *13*(1), 114-133.

Marwick, A., & Lewis, R. (2017). Media manipulation and disinformation online. *Data & Society*. Repéré à https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.

Marzouki, M., & Méadel, C. (2004). De l'organisation des nouveaux collectifs à l'organisation de la cité : gouvernance technique et gouvernement politique d'Internet. *Rapport de recherche de l'Action Spécifique 54 du CNRS-STIC.* Repéré à https://halshs.archives-ouvertes.fr/halshs-00103085

Massit-Folléa, F. (2012). La gouvernance de l'Internet. Une internationalisation inachevée. *Le Temps des médias*, (1), 29-40.

Massit-Folléa, F. (2014). Internet et les errances du multistakeholderism. *Politique étrangère*, (4), 29-41.

Mathieu, L. (2001). *Mobilisations de prostituées*. Paris : Belin.

Mathieu, L. (2002). Rapport au politique, dimensions cognitives et perspectives pragmatiques dans l'analyse des mouvements sociaux. *Revue française de science politique*, *52*(1), 75-100.

Mathieu, L. (2004). Des mouvements sociaux à la politique contestataire : les voies tâtonnantes d'un renouvellement de perspective. *Revue française de sociologie*, *45*(3), 561-580.

Matias, J. N. (2019). The civic labor of online moderators. *Social Media + Society*, *5*(2), 1-12.

Mattoni, A. (2009). Organisation, mobilisation and identity: National and transnational grassroots campaigns between face-to-face and computer-mediated communication. Dans S. Baringhorst, V. Kneip, & J. Niesyto (dir.), *Political campaigning on the Web* (p. 199–231). Bielefeld : Transcript Verlag.

Matusitz, J. (2013). *Terrorism and communication*. Thousand Oaks, CA : Sage Publications.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data : A revolution that will transform how we live, work, and think*. Boston, MA : Houghton Mifflin Harcourt.

McAdam, D. (2010). *Political process and the development of black insurgency, 1930-1970*. Chicago, IL : University of Chicago Press.

McAdam, D., McCarthy, J. D. & Zald, M. N. (1996). Introduction: opportunities, mobilizing structures, and framing processes – toward a synthetic, comparative perspective on social movements. Dans D. McAdam, J. D. McCarthy et M. N. Zald (dir.), *Comparative Perspectives on Social Movements : Political Opportunities, Mobilizing Structures, and Cultural Framings* (p. 1-20). Cambridge : Cambridge University Press.

McAdam, D., Tarrow, C. & Tilly, C. (dir.) (2001). *Dynamics of Contention.* Cambridge : Cambridge University Press.

McCurdy, P. P. (2011). Theorizing" lay theories of media": A case study of the dissent! Network at the 2005 Gleneagles G8 Summit. *International Journal of Communication*, *5*, 619-638.

McLuhan, M. (1964) *Understanding Media: The Extensions of Man.* New York, NY : McGraw-Hill.

Méadel, C., & Sire, G. (2017). Les sciences sociales orientées programmes. *Reseaux*, (6), 9-34.

Meikle, G. (2002). *Future active: Media activism and the Internet*. London & New York : Routledge.

Melucci, A. (1996). *Challenging codes: Collective action in the information age*. Cambridge : Cambridge University Press.

Merari, A. (2015). Du terrorisme comme stratégie d'insurrection. Dans G. Chaliand & A. Blin (dir.), *Histoire du terrorisme : de l'antiquité à Al Qaida* (p.27-71). Villeneuve-d'Ascq : Fayard.

Mercea, D. (2012). Digital prefigurative participation: The entwinement of online communication and offline participation in protest events. *New Media & Society*, *14*(1), 153-169.

Micó, J. L., & Casero-Ripollés, A. (2014). Political activism online: organization and media relations in the case of 15M in Spain. *Information, Communication & Society*, *17*(7), 858-871.

Migaux, P. (2015). Les racines de l'islamisme radical. Dans G. Chaliand et A. Blin (dir.), *Histoire du terrorisme : de l'Antiquité à Daech* (p.341-421). Villeneuve-d'Ascq : Fayard.

Miller, D., & Slater, D. (2000). *Internet*. Oxford : Berg Publishers.

Miller-Idriss, C. (2019). What Makes a Symbol Far Right? Co-opted and Missed Meanings in Far-Right Iconography. Dans M. Fielitz et N. Thruston (dir.), *Post-Digital Cultures of the Far Right* (p. 123-137). Bielefeld : Transcript Verlag.

Milner, R. M. (2013). Pop polyvocality: Internet memes, public participation, and the Occupy Wall Street movement. *International Journal of Communication*, *7*, 2357-2390.

Milner, R. M. (2016). *The world made meme: Public conversations and participatory media*. Cambridge, MA : MIT Press.

Milton, D. (2018). Pulling Back the Curtain: An Inside Look at the Islamic State's Media Organization. *Combating Terrorism Center West Point United States*. Repéré à https://ctc.usma.edu/app/uploads/2018/08/Pulling-Back-the-Curtain.pdf

Mina, A. X. (2014). Batman, Pandaman and the Blind Man: a case study in social change memes and Internet censorship in China. *Journal of Visual Culture*, *13*(3), 359-375.

Mina, A. X. (2019). *Memes to Movements: How the World's Most Viral Media is Changing Social Protest and Power*. Boston, MA : Beacon Press.

Mirzoeff, N. (1998). What is visual culture ? Dans N. Mirzoeff (dir.), *The visual culture reader* (1ère ed., p. 3-13). London & New York : Routledge.

Mirzoeff, N. (2002). The subject of visual culture. Dans N. Mirzoeff (dir.), *The visual culture reader* (2ème ed., p.3-23). London & New York : Routledge.

Mitchell, W. J. T (2011). *Cloning terror: The war of images, 9/11 to the present*. Chicago, IL : University of Chicago Press.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), https://doi.org/10.1177/2053951716679679.

Miyazaki, S. (2012). Algorhythmics: Understanding Micro-Temporality in Computational Cultures. *Computational Culture*, 2. Repéré à http://computationalculture.net/algorhythmics-understanding-micro-temporality-in-computational-cultures/

Mol, A., & Law, J. (2002). Complexities: An introduction. Dans A. Mol et J. Law (dir.), *Complexities : Social Studies of Knowledge Practices* (p. 1-23). Durham, NC : Duke University Press.

Mondzain, M. J. (2002). *L'Image peut-elle tuer ?* Paris : Bayard.

Monnoyer-Smith, L. (2013). Le web comme dispositif : comment appréhender le complexe ? Dans C. Barats (dir.), *Manuel d'analyse du web* (p. 11-31). Malakoff : Armand Colin.

Morelli, A. (2010). *Principes élémentaires de propagande de guerre : Utilisables en cas de guerre froide, chaude ou tiède...* Bruxelles : Éditions Aden.

Morozov, E. (2009a, 19 mai). The brave new world of slacktivism. *Foreign Policy*. Repéré à https://foreignpolicy.com/2009/05/19/the-brave-new-world-of-slacktivism/

Morozov, E. (2009b, 5 septembre). From slacktivism to activism. *Foreign Policy*. Repéré à https://foreignpolicy.com/2009/09/05/from-slacktivism-to-activism/

Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*. New York, NY : Public Affairs.

Morozov, E. V. (2014). *Pour tout résoudre, cliquez ici : l'aberration du solutionnisme technologique*. Limoges : FYP éditions.

Mosca, L., & Della Porta, D. (2009). Unconventional politics online: Internet and the global justice movement. Dans D. Della Porta et M. Diani (dir.), *Democracy in social movements* (p. 194-216). London : Palgrave Macmillan.

Mouffe, C. (2000) *The Democratic Paradox*. London:Verso.

Mouffe, C. (2005). For an Agonistic Public Sphere. Dans L.Tønder and L.Thomassen (dir.), *Radical Democracy: Politics between abundance and lack* (p. 191–205). Manchester: University of Manchester Press.

Mouffe, C. (2010). Politique et agonisme. *Rue Descartes*, (1), 18-24.

Mueller, M. (2010) *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press.

Muhlberger, P. (2004). Running Head: Values in Internet Political Discussion. *Paper presented at the International Communication Association Annual Meeting, New Orleans, 27-31 mai.* Repéré à http://ppc.unl.edu/wp-content/uploads/2019/03/Polarization-of-Political-Attitudes-and-Values-on-the-Internet.pdf

Muniesa, F., Millo, Y., & Callon, M. (2007). An introduction to market devices. *The sociological review*, *55*(2), 1-12.

Murdock, G., & Golding, P. (2004). Dismantling the Digital Divide: Rethinking the Dynamics of Participation and Exclusion. Dans A. Calabrese and C. Sparks (dir.) *Towards a Political Economy of Culture: Capitalism and Communication in the Twenty-first Century* (p. 244–60). Lanham, MD: Rowman & Littlefield.

Murthy, D. (2008). Digital ethnography: An examination of the use of new technologies for social research. *Sociology*, *42*(5), 837-855.

Murthy, D., Powell, A. B., Tinati, R., Anstead, N., Carr, L., Halford, S. J., & Weal, M. (2016). Automation, algorithms, and politics : Bots and political influence: A sociotechnical investigation of social network capital. *International Journal of Communication, 10*, 4952-4971.

Musiani, F. (2012). *Nains sans géants : architecture décentralisée et services Internet.* [thèse de doctorat, École Nationale Supérieure des Mines de Paris]. Pastel. https://pastel.archives-ouvertes.fr/pastel-00795169/document

Musiani, F. (2015). Les architectures P2P : Une solution européenne originale pour la protection des données personnelles?. *Réseaux, 189,* 47-75.

Myers, D. J. (1994). Communication technology and social movements: Contributions of computer networks to activism. *Social Science Computer Review*, *12*(2), 250-260.

Nacos, B. L. (2002). *Mass-mediated terrorism.* Lanham, MD : Rowman & Littlefield Publishers.

Nardi, B., & O'Day, V. (1999). *Information ecologies: Using technology with heart*. Cambridge, MA : MIT Press.

Nasr, W. (2016). *État islamique, le fait accompli*. Paris : Plon.

Nasr, W. (2016, 18 juillet). De la Syrie à l'Afrique, le groupe État islamique affirme continuer à faire des émules. *France 24*. Repéré à https://www.france24.com/fr/20190718-camp-al-hol-syrie-afrique-etat-islamique-ei-continue-attirer-sympathisants

Nelson, P. S., & Scott, J. L. (1992). Terrorism and the media: An empirical analysis. *Economics, 3,* 329–339.

Neveu, E. (1999). Médias, mouvements sociaux, espaces publics. *Réseaux. Communication-Technologie-Société*, *17*(98), 17-85.

Neveu, E. (2010). Médias et protestation collective. Dans E. Agrikoliansky, I. Sommier et O. Fillieule (dir.), *Penser les mouvements sociaux* (p. 245-264). Paris : La Découvete.

Neveu, E. (2015). *Sociologie des mouvements sociaux*. Paris : La Découverte.

Neyland, D. (2015). On organizing algorithms. *Theory, Culture & Society*, *32*(1), 119-132.

Niederer, S., & Van Dijck, J. (2010). Wisdom of the crowd or technicity of content? Wikipedia as a sociotechnical system. *New Media & Society*, *12*(8), 1368-1387.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, *79*, 101-139.

Nissenbaum, A., & Shifman, L. (2017). Internet memes as contested cultural capital: The case of 4chan's/b/board. *New Media & Society*, *19*(4), 483-501.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York, NY : NYU Press.

Norman, D. A. (1999). Affordance, conventions, and design. *Interactions*, *6*(3), 38-43.

Norris, P. (2001) *Digital Divide: Civic Engagement*, *Information Poverty and the Internet World-wide*. Cambridge: Cambridge University Press.

Nguyen, T., Hui, P.-M., Harper, F. M., Terveen, L., & Konstan, J. A. (2014). Exploring the filter bubble: the effect of using recommender systems on content diversity. Dans *Proceedings of the 23rd international conference on World Wide Web* (p. 677-686). Repéré à http://wwwconference.org/proceedings/www2014/proceedings/p677.pdf

Oberschall, A. (1973). Social Conflict and Social Movements. New Jersey, NY : Englewood Cliffs.

Omotoyinbo, F. R. (2014). Online radicalisation: the net or the netizen?. *Socialinės Technologijos*, *4*(01), 51-61.

O'Neil, C. (2016). *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy.* New York, NY : Crown Publishing Group.

Ong, W. (1982) *Orality and Literacy: The Technologizing of the Word.* London & New York : Routledge.

O'Reilly, T. (2005). *What is Web 2.0 : Design patterns and business models for the next generation of sofware.* Repéré à https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html

O'Reilly, T. & Battelle, J. (2004). Opening welcome : The state of the internet industry. *Presented at the Web 2.0 Conference, Hotal Nikko, San Francisco, CA*. Repéré à http://conferences.oreillynet.com/cs/web2con/view/e_sess/5854

Orlikowski, W. J. (2007). Sociomaterial practices: Exploring technology at work. *Organization studies, 28(9), 1435-1448.*

Ostovar, A. (2017). The Visual Culture of Jihad. Dans T. Hegghammer, *Jihadi Culture. The Art and Social Practices of Militant Islamists* (p. 82-127). Cambridge : Cambridge university press.

Paccagnella, L. (1997). Getting the seats of your pants dirty: Strategies for ethnographic research on virtual communities. *Journal of Computer-Mediated Communication*, *3*(1), https://doi.org/10.1111/j.1083-6101.1997.tb00065.x.

Padovani, C. (2010). Citizens' communication and the 2009 G8 Summit in L'Aquila, Italy. *International Journal of Communication*, *4*, 416-439.

Pfaffenberger, B. (1996). "If I Want It, It's OK": Usenet and the (Outer) Limits of Free Speech. *The Information Society*, *12*(4), 365-386.

Paillé, P. (2011). Les conditions de l'analyse qualitative. *SociologieS*, *11*, 1-13.

Paillé, P., & Mucchielli, A. (2016). *L'analyse qualitative en sciences humaines et sociales* (4e éd.). Malakoff : Armand Colin.

Paletz, D. L., & Ayanian, J. Z. a Fozzard, PA (1985). The IRA, the Red Brigades, and the FALN, in the New York Times. *Journal of Communication*, *32*, 167-172.

Papacharissi, Z. (2002). The virtual sphere: The internet as a public sphere. *New media & society*, *4*(1), 9-27.

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. London : Penguin Books.

Park, H. W. (2003). Hyperlink network analysis: A new method for the study of social structure on the web. *Connections*, *25*(1), 49-61.

Passeron, J. C., & Revel, J. (dir.) (2005). *Penser par cas, ou comment remettre les sciences sociales à l'endroit*. Paris : Éditions de l'EHESS

Pasquale, F. (2015). *Black Box Society. Les algorithmes secrets qui contrôlent l'économie et l'information*. Limoges : FYP editions.

Pasquale, F. (2016). Two narratives of platform capitalism. *Yale L. & Pol'y Rev.*, *35*, 309-319.

Pasquinelli, M. (2009). Google's PageRank algorithm: A diagram of cognitive capitalism and the rentier of the common intellect. Dans K. Becker et F. Stalder (dir.), Innsbruck : Studien Verlag.

Pastinelli, M. (1999). Ethnographie d'une délocalisation virtuelle : Le rapport à l'espace des internautes dans les canaux de chat. *In Terminal : technologies de l'information, culture et sociétés*, *79*, 41-60.

Pastinelli, M. (2011). Pour en finir avec l'ethnographie du virtuel ! : Des enjeux méthodologiques de l'enquête de terrain en ligne. *Anthropologie et sociétés*, *35*(1-2), 35-52.

Pearson, E. (2016). The case of roshonara choudhry: Implications for theory on online radicalization, ISIS women, and the gendered jihad. *Policy & Internet*, *8*(1), 5-33.

Peretz, H. (1998). *Les méthodes en sociologie : l'observation*. Paris : La Découverte.

Perrow, C. (1979). The sixties observed. Dans M. Zald et J. Mac Carty, *The dynamics of social movements* (p.192-211). Cambridge, MA : Whinthrop.

Petersen, R. D. (2002). *Understanding Ethnic Violence : Fear, Hatred, and Resentment in Twentieth-Century Eastern Europe*. Cambridge : Cambridge Univeristy Press.

Phillips, W. (2015). *This is why we can't have nice things: Mapping the relationship between online trolling and mainstream culture*. Cambridge, MA : MIT Press.

Phillips, W. (2018). The oxygen of amplification. *Data & Society*. Repéré à https://datasociety.net/output/oxygen-of-amplification/

Phillips, W., & Milner, R. M. (2017). *The ambivalent Internet: Mischief, oddity, and antagonism online*. Hoboken, NJ : John Wiley & Sons.

Piazza, J. A., & Guler, A. (2019). The online caliphate: Internet usage and ISIS support in the Arab world. *Terrorism and Political Violence*. https://doi.org/10.1080/09546553.2019.1606801

Pickerill, J. (2003). *Cyberprotest: Environmental activism online*. Manchester : Manchester University Press.

Pinch, T., & Bijker, W. (1987). The social construction of facts and artifacts: Or how the sociology of science and the sociology of technology might benefit each other. Dans W. E. Bijker, T. P. Hughes et T. Pinch (dir.), *The social construction of technological systems: New directions in the sociology and history of technology* (p. 17-50). Cambridge, MA : MIT Press.

Pires, A. (1997). Échantillonnage et recherche qualitative : essai théorique et méthodologique. Dans J. Poupart, J.-P. Deslauriers, L. H. Groulx, A. R. Lapperrière, Mayer et A. Pires (dir.), *La recherche qualitative : Enjeux épistémologiques et méthodologiques* (p. 113-169). Montréal : Gaëtan Morin.

Pleyers, G. (2013). Le militantisme en réseau. Présentation. *Réseaux*, *181*, 9-21.

Poell, T. (2014). Social media and the transformation of activist communication: Exploring the social media ecology of the 2010 Toronto G20 protests. *Information, Communication & Society*, *17*(6), 716-731.

Postmes, T., & Brunsting, S. (2002). Collective action in the age of the Internet: Mass communication and online mobilization. *Social Science Computer Review*, *20*(3), 290-301.

Postill, J., & Pink, S. (2012). Social media ethnography: The digital researcher in a messy web. *Media International Australia*, *145*(1), 123-134.

Powell, K. A. (2011). Framing Islam: An analysis of US media coverage of terrorism since 9/11. *Communication Studies*, *62*(1), 90-112.

Proulx, S. (2011). L'irruption des médias sociaux : enjeux éthiques et poliques. Dans S. Proulx, M. Millette et L. Heaton (dir.), *Médias sociaux : enjeux pour la communication* (p.9-28). Québec : Presses de l'Université du Québec.

Proulx, S. (2015a). Usages participatifs des technologies et désir d'émancipation : une articulation fragile et paradoxale. *Revue de communication sociale et publique*, (13), 67-77.

Proulx, S. (2015b). Médias et technologie. Dans J. Prud'homme, P. Doray & F. Bouchard (dir.), *Sciences, technologies et sociétés de A à Z* (p.146-158). Montréal : Presses de l'Université de Montréal.

Proulx, S., Millette, M., & Heaton, L. (2011). Introduction. Dans S. Proulx, M. Millette et L. Heaton (dir.), *Médias sociaux : enjeux pour la communication* (p.1-9). Québec : Presses de l'Université du Québec.

Quéré, L. (1992). Le tournant descriptif en sociologie. *Current sociology*, *40*(1), 139-165.

Quéré, L. (1992). L'espace public : de la théorie politique à la métathéorie sociologique. *Quaderni*, *18*(1), 75-92.

Qin, J., Zhou, Y., Reid, E., Lai, G., & Chen, H. (2007). Analyzing terror campaigns on the internet: Technical sophistication, content richness, and Web interactivity. *International Journal of Human-Computer Studies*, *65*(1), 71-84.

Ragin, C.C. (1992). Introduction : Cases of « What is a case ? ». Dans C. C. Ragin, H. S. Becker (dir.), *What is a case?: exploring the foundations of social inquiry* (p. 1-17). Cambridge : Cambridge university press.

Rainie, H., & Wellman, B. (2012). *Networked: The new social operating system*. Cambridge, MA : MIT Press.

Rallet, A., & Rochelandet, F. (2011). La régulation des données personnelles face au web relationnel : une voie sans issue ?. *Réseaux*, (3), 17-47.

Ramsay, G. (2008). Conceptualising online terrorism. *Perspectives on Terrorism*, *2*(7), 3-10.

Rancière, J. (2008). *Le spectateur émancipé*. Paris : La fabrique.

Ratkiewicz, J., Conover, M., Meiss, M. R., Gonçalves, B., Flammini, A., & Menczer, F. (2011). Detecting and tracking political abuse in social media. Dans *Fifth international AAAI conference on weblogs and social media* (p. 297-304). Repéré à http://www.cse.fau.edu/~xqzhu/courses/cap6777/political.abuse.social.media.pdf

Raymond, J. (2006). *Pamphlets and pamphleteering in early modern Britain*. Cambridge : Cambridge University Press.

Reidenberg, J. R. (1996). Governing networks and rule-making in cyberspace. *Emory LJ*, *45*, 911-930.

Rey, M. (2015, 17 mars). Aux origines de l'État islamique. *La vie des idées*. Repéré à http://www.laviedesidees.fr/Aux-origines-de-l-Etat-islamique.html

Renzetti, C. M. (2012). Les défis pratiques et éthiques dans la recherche sur les sujets sensibles. Dans E. Hennequin (dir.), *La recherche à l'épreuve des terrains sensibles : approches en sciences sociales* (p. 11-28). Paris : L'Harmattan.

Rheingold, H. (1993). *The virtual community: Finding commection in a computerized world*. Boston, MA : Addison-Wesley Longman Publishing.

Rheingold, H. (2000). *The virtual community: Homesteading on the electronic frontier*. Cambridge, MA: MIT press.

Rheingold, H. (2003). Smart mobs. *Sociétés*, (1), 75-87.

Richards, I. (2016). "Flexible" capital accumulation in Islamic State social media. *Critical Studies on Terrorism*, *9*(2), 205-225.

Rieder, B., & Smyrnaios, N. (2012). Pluralisme et infomédiation sociale de l'actualité : le cas de Twitter. *Réseaux*, (6), 105-139.

Roberts, L. D. (2015). Ethical issues in conducting qualitative research in online communities. *Qualitative Research in Psychology*, *12*(3), 314-325.

Roberts, S. T. (2019). *Behind the Screen: Content Moderation in the Shadows of Social Media*. New Haven, CT : Yale University Press.

Robey, D., Raymond, B., & Anderson, C. (2012). Theorizing information technology as a material artifact in information systems research. Dans P. M. Leonardi, B. A. Nardi & J. Kallinikos (dir.), *Materiality and organizing: Social interaction in a technological world* (p. 217-236). Oxford : Oxford University Press.

Robinson, L., & Schulz, J. (2009). New avenues for sociological inquiry: Evolving forms of ethnographic practice. *Sociology*, *43*(4), 685-698.

Rogers, R., & Ben-David, A. (2008). The Palestinian—Israeli peace process and transnational issue networks: the complicated place of the Israeli NGO. *New Media & Society*, *10*(3), 497-528.

Romani, V. (2007). Enquêter dans les Territoires palestiniens. *Revue française de science politique*, *57*(1), 27-45.

Rolfe, B. (2005). Building an electronic repertoire of contention. *Social Movement Studies*, *4*(1), 65-74.

Rose, G. (2006). *Visual methodologies: An introduction to interpreting visual materials*. Thousand Oaks, CA : SAGE.

Rougier, B. (2016a). Introduction. Dans B. Rougier (dir), *Qu'est-ce que le salafisme* (p.1-25). Paris : PUF.

Rougier, B. (2016). Le jihad en Afghanistan et l'émergence du salafisme-jihadisme. Dans B. Rougier (dir), *Qu'est-ce que le salafisme* (p.65-87). Paris : PUF.

Rouvroy, A. (2011). Technology, virtuality and utopia: Governmentality in an age of autonomic computing. Dans M. Hildebrandt et A. Rouvroy (dir.), *Law, human agency and autonomic computing* (p. 135-156). London & New York : Routledge.

Rouvroy, A., & Berns, T. (2013). Gouvernementalité algorithmique et perspectives d'émancipation. *Réseaux*, (1), 163-196.

Roy, O. (2001). *Généalogie de l'islamisme.* Paris : Pluriel.

Roy, O. (2016). *Le djihad et la mort*. Le Seuil.

Roy, N., & Garon, R. (2013). Hors thème Étude comparative des logiciels d'aide à l'analyse de données qualitatives : de l'approche automatique à l'approche manuelle. *Recherches qualitatives*, *32*(1), 154-180.

Rudner, M. (2017). "Electronic Jihad": The Internet as Al Qaeda's Catalyst for Global Terror. *Studies in Conflict & Terrorism*, *40*(1), 10-23.

Ruppert, E., Law, J., & Savage, M. (2013). Reassembling social science methods: The challenge of digital devices. *Theory, culture & society*, *30*(4), 22-46.

Ryan, C. (1991). *Prime time activism : Media strategies for grasstroots organizing*. Boston, MA : South End Press.

Saltman, E. M., & Winter, C. (2014). Islamic state: The changing face of modern jihadism. *Quilliam Foundation.* Repéré à : https://www.quilliaminternational.com/shop/e-publications/islamic-state-the-changing-face-of-modern-jihadism-2/

Sassen, S. (2002). Towards a sociology of information technology. *Current Sociology*, *50*(3), 365-388.

Savage, M. (2009). Contemporary sociology and the challenge of descriptive assemblage. *European Journal of Social Theory*, *12*(1), 155-174.

Savage, M., & Burrows, R. (2007). The coming crisis of empirical sociology. *Sociology*, *41*(5), 885-899.

Schäfer, M. T. (2011). *Bastard culture!: how user participation transforms cultural production*. Amsterdam : Amsterdam University Press.

Schäfer, F., Evert, S., & Heinrich, P. (2017). Japan's 2014 General Election: Political Bots, Right-Wing Internet Activism, and Prime Minister Shinzō Abe's Hidden Nationalist Agenda. *Big data*, *5*(4), 294-309.

Scheufele, D. A., & Nisbet, M. C. (2002). Being a citizen online: New opportunities and dead ends. *Harvard International Journal of Press/Politics*, *7*(3), 55-75.

Schmid, A. & de Graaf, J. (1982). *Violence as Communication: Insurgent Terrorism and the Western News Media.* Thousand Oaks, CA : SAGE.

Schradie, J. (2019). *The Revolution that Wasn't: How Digital Activism Favors Conservatives*. Cambridge, MA : Harvard University Press.

Selwyn, N. (2004). Reconsidering political and popular understandings of the digital divide. *New media & society*, *6*(3), 341-362.

Selnow, G.W. (1998) *Electronic Whistle-stops:The Impact of the Internet on American Politics*. Westport & London : Praeger.

Serghini, Z. B., & Matuszak, C. (2009). Lire ou relire Habermas : lectures croisées du modèle de l'espace public habermassien. *Études de communication. langages, information, médiations*, (32), 33-49.

Shane, M. P. (2004). *Democracy online: the prospects for political renewal through the Internet*. London & New York : Routledge.

Shapiro, A. (1999) *The Control Revolution: How the Internet Is Putting Individuals in Charge and Changing the World as We Know it*. New York, NY : Public Affairs.

Shifman, L. (2013a). *Memes in digital culture.* Cambridge, MA: MIT Press.

Shifman, L. (2013b). Memes in a digital world: Reconciling with a conceptual troublemaker. *Journal of Computer-Mediated Communication*, *18*(3), 362-377.

Shirky, C. (2008). *Here comes everybody: The power of organizing without organizations*. London : Penguin Books.

Shirky, C. (2011). The political power of social media: Technology, the public sphere, and political change. *Foreign affairs*, 28-41.

Shohat, E. & Stam, R. (1998). Narrativizing visual culture : towards a polycentric aesthetic. Dans N. Mirzoeff (dir.), *The visual culture reader* (1e éd., p. 27-49). London & New York : Routledge.

Simondon, G. (1958). *Du mode d'existence des objets techniques*. Paris : Aubier.

Singer, P. & Brooking T. (2018). *Likewar : The weaponization of social media*. Boston, MA : Houghton Mifflin Harcourt

Slingeneyer, T. (2007). La nouvelle pénologie, une grille d'analyse des transformations des discours, des techniques et des objectifs dans la pénalité. *Champ pénal/Penal field*, *4*, 1-25.

Small, T. A. (2011). What the hashtag? A content analysis of Canadian politics on Twitter. *Information, communication & society*, *14*(6), 872-895.

Snow, D. A. (2001). Analyse de cadres et mouvements sociaux. Dans D. Cefaï et D. Trom (dir.), *Les formes de l'action collective* (p. 1-21). Paris : Éditions de l'EHESS.

Snow, D. A., Rochford, E. B., Worden, S. K., & Benford, R. D. (1986). Frame alignment processes, micromobilization, and movement participation. *American sociological review*, 464-481.

Snow, D. A., & Benford, R. D. (1988). Ideology, frame resonance, and participant mobilization. *International social movement research*, *1*(1), 197-217.

Snow, D. A., & Benford, R. D. (1992). Master frames and cycles of protest. Dans A. D. Morris et C. McClurg Mueller, *Frontiers in social movement theory*, (133-155). New Haven, CT : Yale University Press.

Sommier, I. (2009). Émotions. Dans O. Fillieule, L. Mathieu et C. Péchu (dir.), *Dictionnaire des mouvements sociaux* (p. 197-206). Paris : La Découverte.

Sommier, I. (2010). Les états affectifs ou la dimension affectuelle des mouvements sociaux. Dans E. Agrikoliansky, I. Sommier et O. Fillieule, *Penser les mouvements sociaux* (p.185-202). Paris : La Découvete.

Sommier, I. (2015). Sentiments, affects et émotions dans l'engagement à haut risque. *Terrains/Théories*, (2). Repéré à : https://journals.openedition.org/teth/236.

Song, F. W. (2010). Theorizing web 2.0: A cultural perspective. *Information, Communication & Society*, *13*(2), 249-275.

Sorel, J. M. (2002). Existe-t-il une définition universelle du terrorisme ? Dans K. Bannelier, T. Christakis, O. Corten et B. Delcourt (dir.), *Le Droit international face au terrorisme* (p. 35-68). Paris : Editions A. Pedone.

Sotlar, A. (2004). Some Problems with a Definition and Perception of Extremism within a Society. Dans G. Mesko, M. Pagon et B. Dobovsek (dir.), *Policing in central and Eastern Europe: Dilemmas of contemporary criminal justice*, 7(p. 703-707). University of Maribor, Slovenia. Repéré à https://www.ncjrs.gov/pdffiles1/nij/Mesko/208033.pdf

Soulé, B. (2007). Observation participante ou participation observante ? Usages et justifications de la notion de participation observante en sciences sociales. *Recherches qualitatives*, *27*(1), 127-140.

Sourdel, J., & Sourdel, D. (1996). Dictionnaire historique de l'islam. Paris : PUF.

Srnicek, N. (2017). *Platform capitalism*. Hoboken, NJ : John Wiley & Sons.

Srinivasan, R., & Fish, A. (2011). Revolutionary tactics, media ecologies, and repressive states. *Public Culture*, *23*(3 (65)), 505-510.

Standage, T. (2013). *Writing on the wall: Social media-The first 2,000 years*. London : Bloomsbury Publishing.

Star, S. L., & Griesemer J. R. (1989). Institutional ecology, "translations" and boundary objects: Amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907–39. *Social Studies of Science* 19 (3):387–420.

Star, S. L. (1999). The Ethnography of Infrastructure. *American Behavioral Scientist, 43*(3), p. 377-391.

Star, S. L. (2018). L'ethnographie des infrastructures. *Tracés. Revue de Sciences humaines*, (35), 187-206.

Stein, L. (2009). Social movement web use in theory and practice: A content analysis of US movement websites. *New Media & Society*, *11*(5), 749-771.

Stern, J. & Berger, J.M. (2016). *ISIS : The State of Terror.* New York, NY : Ecco Press.

Steuter, E. (1990). Understanding the media/terrorism relationship: An analysis of ideology and the news in Time magazine. *Political Communication*, *7*(4), 257-278.

Stromer-Galley, J. (2002). New voices in the public sphere: A comparative analysis of interpersonal and online political talk. *Javnost-The Public*, *9*(2), 23-41.

Stukal, D., Sanovich, S., Bonneau, R., & Tucker, J. A. (2017). Detecting bots on Russian political Twitter. *Big data*, *5*(4), 310-324.

Suchman, L. (2007). *Human-machine reconfigurations: Plans and situated actions*. Cambridge : Cambridge university press.

Suchman, L. (2000). Organizing alignment: A case of bridge-building. *Organization*, *7*(2), 311-327.

Suchman, L. (2012). Configuration. Dans N. Wakeford et C. Lury (dir.), *Inventive methods* (p. 62-74). London & New York : Routledge.

Sustein, C. R. (2007). *Republic. com 2.0*. Princeton : Princeton University Press.

Sveningsson, M. (2004). Ethics in Internet ethnography. Dans E. A. Buchanan (dir.), *Readings in virtual research ethics: Issues and controversies* (p. 45-61). Hershey & London : Information Science Publishing

Tarde (1893). *La logique sociale*. Paris : Les Empêcheurs de penser en rond.

Tarde (1985). *Monadologie et sociologie*. Paris : Les Empêcheurs de penser en rond.

Tarrow, S. (1985). Democracy and Disorder. Protest and Politics in Italy, 1965-1975. Oxford : Oxford University Press.

Tarrow, S. (1994). *Power in movement: Social movements and contentious politics*. Cambridge : Cambridge University Press.

Taylor, V., & Whittier, N. (1995). Analytical approaches to social movement culture: The culture of the women's movement. Dans H. Johnston (dir.), *Social movements and culture* (p.163-187). Minneapolis, MN : University of Minnesota Press.

Theocharis, Y. (2013). The wealth of (occupation) networks? Communication patterns and information distribution in a Twitter protest network. *Journal of Information Technology & Politics*, *10*(1), 35-56.

Théron, J. (2015, février). Funeste rivalité entre Al-Qaida et l'Organisation de l'État islamique. *Le monde diplomatique*. Repéré à https://www.monde-diplomatique.fr/2015/02/THERON/52632.

Thévenot, L. (1993). Essai sur les objets usuels. Dans B. Conein, N. Dodier et L. Thévenot (dir.), *Les objet dans l'action : De la maison au laboratoire* (p. 85-115). Paris : Raisons pratiques.

Thévenot, L. (2006). *L'action au pluriel : sociologie des régimes d'engagement*. Paris : La Découverte.

Thoër, C., Millerand, F., Myles, D., Orange, V., & Gignac, O. (2012). Enjeux éthiques de la recherche sur les forums Internet portant sur l'utilisation des médicaments à des fins non médicales. *Communiquer. Revue de communication sociale et publique*, (7), 1-22.

Thomas, R. (1996). Access and Inequality. Dans N. Heap, R. Thomas, G. Einon, R. Mason et H. Mackay (dir.), *Information Technology and Society*, (p. 90–100). Thousand Oaks, CA : SAGE.

Thomas, D. (2016). Le rôle d'Internet dans la diffusion de la doctrine salafiste. Dans B. Rougier (dir), *Qu'est-ce que le salafisme* (p.87-105). Paris : PUF.

Thompson, J.B. (1995). *The Media and Modernity : A Social Theory of the Media*. Cambridge : Polity.

Thompson, J. B. (2000). Transformation de la visibilité. *Réseaux*, *18*(100), 187-213.

Thompson, J. B. (2005). La nouvelle visibilité. *Réseaux*, *129*(1), 59-87.

Thomson, D. (2014). *Les français jihadistes*. Paris : Les Arènes.

Thomsen, S. R., Straubhaar, J. D., & Bolyard, D. M. (1998). Ethnomethodology and the study of online communities: exploring the cyber streets. *Information research*, *4*(1), 4-1.

Thrift, N. (2004). Remembering the technological unconscious by foregrounding knowledges of position. *Environment and planning D: Society and space*, *22*(1), 175-190.

Tilly, C. (1978). *From mobilization to revolution*. Massachusetts, MA : Addison-Wesley Publishing Company.

Tilly, C. (1984) Social movements and national politics. Dans C. Bright et S. Harding (dir.), *Statemaking and Social Movements: Essays in History and Theory* (p. 297-317). Ann Arbor, MI : University of Michigan Press.

Tilly, C. (1986). *La France conteste. De 1600 à nos jours*. Paris : Fayard.

Tilly, C. (1995). Contentions Repertoires in Great Britain, 1758-1834. Dans M. Traugott (ed.), *Repertoires and Cycles of Collective Action* (p. 15-42). Durham, NC : Duke University Press.

Torres Soriano, M. R. (2010). The road to media Jihad: The propaganda actions of al Qaeda in the Islamic Maghreb. *Terrorism and Political Violence*, *23*(1), 72-88.

Torres, M. R., Jordán, J., & Horsburgh, N. (2006). Analysis and evolution of the global jihadist movement propaganda. *Terrorism and Political Violence*, *18*(3), 399-421.

Traïni, C. (2008). *S'émouvoir pour la cause*. Paris : Presses de Sciences Po.

Traïni, C. (2009) (dir.). *Émotions… Mobilisation !*. Paris : Presses de Sciences Po.

Traïni, C. (2009). Introduction. Pourquoi et comment sensibiliter à la cause ?. Dans C. Traïni (dir.), *Émotions… Mobilisation !* (p. 11-34). Paris : Presses de Sciences Po.

Tréguer, F. (2017). Pouvoir et résistance dans l'espace public : une contre-histoire d'Internet (XV^{e}-XXi^{e} siècle). [thèse de doctorat, l'EHESS]. HALSHS https://halshs.archives-ouvertes.fr/tel-01631122v2/document.

Treré, E. (2012). Social movements as information ecologies: Exploring the coevolution of multiple Internet technologies for activism. *International Journal of Communication*, *6*, 19.

Treré, E. (2018). *Hybrid media activism: Ecologies, imaginaries, algorithms*. London & New York : Routledge.

Treré, E., & Mattoni, A. (2016). Media ecologies and protest movements: main perspectives and key lessons. *Information, Communication & Society*, *19*(3), 290-306.

Trudel, P. (2000). Quel droit et quelle régulation dans le cyberespace ?. *Sociologie et sociétés*, *32*(2), 190-210.

Trudel, P. (2006). L'encadrement normatif des technologies : une gestion réseautique des risques. *Rapport présenté au 30e congrès de l'Institut international de droit d'expression et d'inspiration françaises.* Repéré à https://papyrus.bib.umontreal.ca/xmlui/handle/1866/702.

Tsfati, Y., & Weimann, G. (2002). www. terrorism. com: Terror on the Internet. *Studies in Conflict and Terrorism*, *25*(5), 317-332.

Tufekci, Z. (2013). "Not this one" social movements, the attention economy, and microcelebrity networked activism. *American Behavioral Scientist*, *57*(7), 848-870.

Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. New Haven, CT : Yale University Press.

Tufekci, Z., & Wilson, C. (2012). Social media and the decision to participate in political protest: Observations from Tahrir Square. *Journal of communication*, *62*(2), 363-379.

Tuman, J. S. (2009). *Communicating terror: The rhetorical dimensions of terrorism*. Thousand Oaks, CA : Sage Publications.

Turow, J. (2012). *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*. New Haven, CT: Yale University Press.

Van Aelst, P., & Walgrave, S. (2002). New media, new movements? The role of the internet in shaping the 'anti-globalization'movement. *Information, Communication & Society*, *5*(4), 465-493.

Van Atta, D. (1998). Carbombs and cameras: The need for responsible media coverage of terrorism. *Harvard International Review, Fall,* 66–70.

Van Deursen, A., & Van Dijk, J. (2011). Internet skills and the digital divide. *New media & society*, *13*(6), 893-911.

Van Deursen, A. J., & Van Dijk, J. A. (2014). The digital divide shifts to differences in usage. *New media & society*, *16*(3), 507-526.

Van Deursen, A. J., & van Dijk, J. A. (2019). The first-level digital divide shifts from inequalities in physical access to inequalities in material access. *?ew media & society*, *21*(2), 354-375.

Van Dijck, J. (2013). *The culture of connectivity: A critical history of social media*. Oxford : Oxford University Press.

Van Dijck, J., Poell, T., & De Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford : Oxford University Press.

Van Dijk, J. A. (2006). Digital divide research, achievements and shortcomings. *Poetics*, *34*(4-5), 221-235.

Van Dijk, J., & Hacker, K. (2003). The digital divide as a complex and dynamic phenomenon. *The information society*, *19*(4), 315-326.

Van Eeten, M. J., & Mueller, M. (2012). Where is the governance in Internet governance?. *New Media & Society*, (0), 1-17.

Van Laer, J. (2010). Activists ‘online’ and ‘offline’: The Internet as an information channel for protest demonstrations. *Mobilization* 15(3): 405–417.

Van Laer, J., & Van Aelst, P. (2009). Cyber-protest and civil society: the Internet and action repertoires in social movements. Dans Y. Jewkes (dir.), *Handbook on internet crime* (p. 230-255). Cullompton & Portland : Willan publishing.

Van Laer, J., & Van Aelst, P. (2010). Internet and social movement action repertoires: Opportunities and limitations. *Information, Communication & Society*, *13*(8), 1146-1171.

Van den Boomen, M. (dir.) (2009). *Digital material: Tracing new media in everyday life and technology* (Vol. 2). Amsterdam : Amsterdam University Press.

Van der Nagel, E. (2018). ‘Networks that work too well’: intervening in algorithmic connections. *Media International Australia*, *168*(1), 81-92.

Van de Donk W., Loader B.D., Nixon P.G. and Rucht D. (2004) *Cyberprotest: New Media and Social Movements*. London & New York : Routledge.

Vaidhyanathan, S. (2018). *Antisocial media: How Facebook disconnects us and undermines democracy*. Oxford : Oxford University Press.

Vale, G. (2018). Cubs in the Lions’ Den : Indoctrination and Recruitment of Children Within Islamic State Territory. *The International Centre for the Study of Radicalisation (ICSR)*. Repéré à https://icsr.info/2018/07/23/cubs-in-the-lions-den-indoctrination-and-recruitment-of-children-within-islamic-state-territory/.

Venturini, T., Cardon, D., & Cointet J.-P. (2014). Présentation. *Réseaux, 6*(188), 9-21.

Vīķe-Freiberga, V., Däubler-Gmelin, H., Hammersley, B., & Maduro, M.P, (2013). A free and pluralistic media to sustain European democracy. *High Level Expert Group on Media Freedom and Pluralism.* Repéré à https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/HLG%20Final%20Report.pdf

Volkoff, O., Strong, D. M., & Elmes, M. B. (2007). Technological embeddedness and organizational change. *Organization science*, *18*(5), 832-848.

Von Behr, I., Reding, A., Edwards, C., & Gribbon, L. (2013). Radicalisation in the Digital Era-The use of the internet in 15 cases of terrorism and extremism. *Rand Europe*. Repéré à https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

Von Hippel, E. (1988). *The Sources of Innovation*. Oxford : Oxford University Press.

Voirol, O. (2005a). Présentation. Réseaux,(129–130), 9–36.

Voirol, O. (2005b). Les luttes pour la visibilité. *Réseaux*, (1), 89-121.

Weimann, G. (2004). www. terror. net: How modern terrorism uses the Internet. *United States Institute of Peace Special Report.* Repéré à https://www.usip.org/sites/default/files/sr116.pdf

Weimann, G. (2016). The emerging role of social media in the recruitment of foreign fighters. Dans A. de Guttry, F. Capone et C. Paulussen (dir.), *Foreign fighters under international law and beyond* (p. 77-95). Berlin : Springer

Wieviorka, M., & Wolton, D. (1987). *Terrorisme à la une : média, terrorisme et démocratie*. Paris : Gallimard.

Whine, M. (1999). Cyberspace-a new medium for communication, command, and control by extremists. *Studies in Conflict and Terrorism*, *22*(3), 231-245.

Wignell, P., Tan, S., O'Halloran, K. L., & Lange, R. (2017). A mixed methods empirical examination of changes in emphasis and style in the extremist magazines Dabiq and Rumiyah. *Perspectives on Terrorism*, *11*(2), 2-20.

Williams, R. (dir.) (1981) *Contact: Human Communication and Its History.* New York, NY: Thames and Hudson.

Wilkinson, P. (1997). The media and terrorism: a reassessment. *Terrorism and political violence*, *9*(2), 51-64.

Willson, M. (2017). Algorithms (and the) everyday. *Information, Communication & Society*, *20*(1), 137-150.

Winner, L. (1980). Do Artifacts have Politics? *Deadalus, 109*(1), 121-136.

Winter, C. (2015). Documenting the virtual " caliphate ". *Quilliam Fondation*. Repéré à http://www.quilliamfoundation.org/wp/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf

Winter, C. (2018). Apocalypse, later: a longitudinal study of the Islamic State brand. *Critical Studies in Media Communication*, *35*(1), 103-121.

Witschge, T. (2004). Online deliberation: Possibilities of the Internet for deliberative democracy. Dans P. M. Shane (dir.), *Democracy online: the prospects for political renewal through the Internet* (p. 129-142). London & New York : Routledge.

Woolgar, S. (1991). Configuring the user: The case of usability trials. Dans J. Law (dir.), *A Sociology of Monsters* (p. 57-99). London & New York : Routledge.

Woolgar, S. (2002) *Virtual Society? Technology, Cyberbole, Reality*. Oxford : Oxford University Press.

Woolley, S. C. (2016). Automating power: Social bot interference in global politics. *First Monday*, *21*(4).

Woolley, S. C., & Howard, P. N. (2016a). Social media, revolution, and the rise of the political bot. Dans P. Robinson, P. Seib, et R. Frohlich (dir.), *Routledge handbook of media, conflict, and security* (p. 282–292). London & New York : Routledge.

Woolley, S. C., & Howard, P. N. (2016b). Automation, algorithms, and politics| Political communication, computational propaganda, and autonomous agents—Introduction. *International Journal of Communication*, *10*, 4882-4890.

Woolley, S. C., & Howard, P. N. (2017). Computational propaganda worldwide: Executive summary. *Working Paper 2017.11. Oxford, UK: Project on Computational Propaganda.* Repéré à http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

Wu, T. (2017). *The attention merchants: The epic scramble to get inside our heads*. New York, NY : Vintage Books.

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, *12*(4), 505-523.

Yin, R. K. (2003). *Case study research and applications: Design and methods*. Thousand Oaks, CA : SAGE.

Zelin, A. Y. (2015). Picture or it didn't happen: A snapshot of the Islamic State's official media output. *Perspectives on Terrorism*, *9*(4), 85-97.

Zhang, J., Carpenter, D., & Ko, M. (2013). Online astroturfing: A theoretical perspective. Dans *19th Americas Conference on Information Systems (AMCIS) Proceedings*. Repéré à https://www.researchgate.net/publication/286729041_Online_astroturfing_A_theoretical_perspective.

Zittrain, J. (2008). *The future of the Internet – And How to stop it.* New Haven, CT : Yale University Press.

Ziewitz, M., & Brown, I. (2013). A prehistory of internet governance. Dans I. Brown (dir.), *Research Handbook on Governance of the Internet* (p.3-27). Cheltenham : Edward Elgar Publishing.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75-89.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London : Profile Books.

ANNEXE 1. Présentation de l'État islamique[129]

L'avènement de l'État islamique n'est pas le fruit d'un hasard, mais découle d'un long processus qui a su profiter de plusieurs instabilités politiques pour établir à leur Califat (Atran, 2016). Quand en 2003 les forces américaines ont destitué Sadam Hussein de ses fonctions s'en est suivie une situation de chaos qui aura servi d'incubateur à un nouveau jeu politique marqué par l'émergence de formes multiples de violence (El Difraoui, 2016 ; Rey, 2015). C'est à ce moment que le Jordanien Moussad al-Zarqawi fait son entrée en transférant en Irak les activités de son groupe international *Jammaat Al-Tawhdid Wal-Djihad* (Théron, 2015). En 2004, le groupe porte allégeance à Ben Laden et devient Al-Qaïda en Irak, ou plus précisément Al-Qaïda au pays des deux fleuves. Rapidement, leur doctrine se distancie de celle de la maison mère : la priorité est maintenant celle de l'ennemi proche, plutôt qu'un rival éloigné, comme les États-Unis ou Israël (Harling, 2014 ; Hénin, 2015).

Accordant de moins en moins d'importance à l'occupant américain, ils provoquent une guerre confessionnelle entre sunnites et chiites, pour ensuite s'inscrire dans une logique fratricide. Quelques mois après qu'al-Zarqawi ait été tué par les Américains en juin 2006, Al-Qaïda en Irak deviendra progressivement l'État islamique en Irak, avec Abou Omar al-Baghdadi (2006-2010) et puis Abou Bakr Al-Baghdadi (2010-2019)[130] à sa tête. Durant ces années en Irak, le groupuscule s'est principalement efforcé de croître en intégrant des combattants étrangers et des groupes tribaux locaux (Rey, 2015). La guerre en Syrie bouleversera la donne et constituera un terrain propice à l'expansion du groupe. En 2012, L'État islamique en Irak a commencé à s'étendre en Syrie, grâce notamment à Haji Bakr qui a joué un rôle primordial dans l'infiltration du groupe en Syrie, avec la création de cellules d'espions dans des villes et des villages et des campagnes d'assassinats et d'enlèvements ciblés (Chaliand, 2015). L'entrée sur le terrain syrien a été officialisée en 2013, lorsque l'État islamique en Irak devient l'État islamique en Irak et au Levant, puis simplement l'État islamique. Pour accroître son implantation, l'organisation a effectué une offensive éclair en 2014, entre d'une part la prise de Mossoul et d'autre part l'autoproclamation de l'émir Abou Bakr Al-Baghdadi en calife de l'État islamique. Il demandera allégeance à Ayman al-Zawahiri – chef d'Al-Qaïda – que ce dernier refusera.

Même si, tout comme Al-Qaïda, l'État islamique se base sur la fraternité des combattants et l'appel à un jihadisme mondial où l'*Umma* transcende toute autre structure sociale, ce mouvement conquérant s'est construit sur une identité claire qui diverge sur certains points de celle d'Al-Qaïda (Théron, 2015). La principale caractéristique réside dans le fait que l'État islamique cherche avant tout à stabiliser géographiquement le mouvement, en s'installant sur un territoire permanent (Luizard, 2017). La stratégie d'Al-Qaïda a toujours été de déstabiliser un État, sans pour autant en établir son administration directe, au contraire de l'État islamique qui recherche à affirmer sa souveraineté sur un territoire. Comme l'explique l'auteur, la

[129] Cette section présente dans les grandes lignes la genèse du groupe État islamique, mais n'a pas pour prétention d'en faire l'exhaustivité. Le lecteur désireux d'en connaître plus pourra se référer aux ouvrages suivants : Atran, S. (2016). *L'État islamique est une révolution*. Paris : Les liens qui libèrent ; Luizard, P.-J. (2017). *Le piège Daech : L'État islamique ou le retour de l'Histoire.* Paris : La Découverte ; Stern, J. & Berger, J.M. (2016). *ISIS : The State of Terror.* New York, NY : Ecco Press ; Nasr, W. (2016). *État islamique, le fait accompli*. Paris : Plon.

[130] Abou Bakr al-Baghdadi a d'abord été Émir de l'État islamique en Irak et au Levant (2010-2014) pour ensuite devenir Calife de l'État islamique (2014-2019). Il a été tué en ocotobre 2019 à Baricha, en Syrie, à la suite d'une opération américaine. Son successeur est Abi Ibrahim Al-Hachimi Al-Qourachi.

stratégie de l'organisation islamique a pour but ultime une domination claire sur tous : sunnites modérés, chiites, alaouites, chrétiens, juifs, yézidis. La lutte contre le chiisme et les Kurdes jugés impies et la supériorité de l'organisation sur les autres croyances forment un fondement idéologique pour l'organisation, contrairement à Al-Qaïda qui s'est constitué à partir de motivations anti-occidentales.

En octobre 2014 le groupe a atteint son apogée en contrôlant près de 60 000 km^2 des territoires syriens et irakiens (Breteau, 2019). Il a aussi réussi à s'emparer de grandes villes comme Raqqa et Mossoul, ainsi qu'à assurer son autonomie financière (Nasr, 2016). Une partie de son succès tient à sa stratégie de conquête qui est loin de découler d'une improvisation. L'organisation suit des stratégies de contrôle et d'expansion déployées dans des documents qui forment son corpus de référence. Parmi ceux-ci, l'opuscule rédigé entre 2002 et 2004 par un théoricien jihadiste sous le pseudonyme d'Abu Bakr al-Naji intitulé « *l'administration de la sauvagerie : l'étape la plus critique à franchir par la Oumma* ». Cet opuscule explique précisément la stratégie à adopter par les groupes jihadistes pour qu'ils puissent s'implanter territorialement face aux régimes arabes et musulmans d'une part, et face aux Américains et Occidentaux, d'autre part.

Le livre indique que le groupe jihadiste doit s'accaparer des régions en proie à l'anarchie et au chaos, dans lesquelles ils devront gagner le soutien populaire en se montrant comme étant la seule alternative possible. Il faut ensuite que le groupe jihadiste gère ce chaos conformément à un schéma de construction étatique hobbesien, c'est-à-dire en rétablissant la sécurité et les services sociaux, en distribuant de la nourriture et des médicaments et en prenant en charge l'administration des territoires (Glasman, 2014). Pour multiplier les régions administrées par les jihadistes, Naji formule une série de recommandations que doivent prendre les groupes : développer la religiosité des masses ; faire de la religion l'ordre social et politique ; former militairement les jeunes. En parallèle, l'auteur appelle aussi les adhérents à lutter contre le « halo trompeur » des médias occidentaux et à produire leurs propres médias qui diraient la « vérité ». Pour ce faire, Naji recommande aux jihadistes d'étudier en profondeur les médias occidentaux pour comprendre comment employer leurs propres outils de façon optimale.

Le succès territorial de l'État islamique s'est toutefois terni au cours des dernières années, à la faveur des combats opposés (forces kurdes, irakiennes, syriennes, coalition, etc.). Malgré le déclin majeur de la superficie de ces zones syro-irakiennes, le groupuscule jihadiste reste attractif et prolifère sur plusieurs continents. En juillet 2019, le groupe a par exemple diffusé une vidéo montrant un drapeau noir hissé par des partisanes en plein milieu du camp d'Al-Hol, dans le nord-est de la Syrie. Ce cas n'est pas isolé, à la mi-juillet neuf vidéos en faveur de l'État islamique en également été diffusée sur internet montrant la présence des jihadistes dans quinze pas dont la Turquie, l'Inde, le Mali, les Philippines, la Libye, l'Égypte, la Somalie, le Yémen, le Mozambique ou encore le Cameroun (Nasr, 2019).

ANNEXE 2. The Table of the Statistics for the Video Releases Video Realeses[131]

Number	Wilayah [name], video name	Scenario, idea and comment - Out of 30%	Professional filming and quality of raw materials - Out of 30%	Montage, graphics, effects, editing and scenes choosing - Out of 40%	Final result - Out of 100%
1	Wilayat al-Khayr - Light and Heavy	25	20	15	60 Very good
2	Wilayat al-Janub - The Monthly Statistics	10	0	25	35 Weak
3	Wilayat al-Jazirah - Aspect of the Course of Battles	10	15	15	45 Acceptable
4	Wilayat al-Fallujah - And Give Glad Tidings to the Patient Ones	25	20	25	70 Very good
5	Wilayat al-Furat - The Greatest Losers	25	25	20	70 Very good
6	Wilayat al-Furat - Guardians of the Citizens	25	20	20	65 Very good
7	Wilayat al-Raqqah - And Allah will Enrich You from His Blessings	20	25	25	70 Very good
8	Wilayat Dijlah - The Assembly will be Defeated and They will Turn Their Backs in Retreat	20	15	15	50 Good
9	Wilayat Hama - Fight Them for They are Polytheists	25	10	15	50 Good
10	Wilayat Baghdad - For They will Kill and Then be Killed	15	10	15	40 Acceptable
11	Wilayat al-Fallujah - Where to Escape?	30	30	30	90 Excellent
12	Wilayat Kirkuk - The Attack Against Barracks of the Rafidi Mobilization	10	15	15	40 Acceptable
13	Wilayat Salahuddin - The Attackers	20	25	35	80 Excellent
14	Wilayat Salahuddin - The Clashing of Sowrds	20	20	30	70 Very good
15	Wilayat Ninawa - Abundant Provision	25	20	20	65 Very good
16	Wilayat Ninawa - Glad Tidings in the Support of the Tribes	25	20	25	70 Very good
17	Wilayat Aleppo - Invading Villages to Spread the Guidance	30	30	35	95 Excellent
18	Wilayat al-Anbar - With Patience and Certainty You will be Granted Victory	25	20	25	70 Very good
19	Wilayat al-Jazirah - Sinai, the Pride and Rebellions	20	15	15	50 Good
20	Wilayat al-Furat - And You will be the Superior Ones	20	20	25	65 Very good
21	Wilayat al-Fallujah - With Hardship will be Ease	30	20	25	75 Excellent
22	Wilayat Aleppo - From Aleppo to Sinai	25	20	20	65 Very good
23	Wilayat Hama - A Message to Our Brothers in Sinai	20	15	15	50 Good
24	Wilayat Homs - Sinai, The Gateway to Jerusalem	20	15	15	50 Good
25	Wilayat Dijlah - Sinai, the Pride and Steadfastness	20	10	20	50 Good
26	Wilayat Damascus - Sinai, the Land of Epic Battles and Sacrifice	10	5	10	25 Weak
27	Wilayat Salahuddin - Messages of Steadfastness to the Land of Declamation	25	20	25	70 Very good
28	Wilayat Kirkuk - The Descendants of the [Prophet] Companions Have Returned	20	10	20	50 Good
29	Wilayat Ninawa - Sinai, Have Patience for Victory is Coming	25	15	30	70 Very good
30	Wilayat al-Khayr - The Sparkle of Sword and Hope	20	20	30	70 Very good
31	Wilayat Tripoli - And the Best Outcome is for the Righteous	25	20	20	65 Very good
32	Wilayat al-Janub - The Raid of Abu Sabah al-Zuba`i	20	20	25	65 Very good
33	Wilayat al-Raqqah - Destroy It	30	20	25	75 Excellent
34	Wilayat al-Jazirah - The Brutal Killing of the Agents of the Cross	20	20	20	60 Very good

Note: The top quality video releases are those that gain 70% or more

The Final Score:

- The number of video releases: 34
- The number of top quality releases: 14
- The number of excellent releases: 5
- The number of very good releases: 17
- The number of good releases: 8
- The number of acceptable releases: 4

And God is He Who Grant Success and He Guides for the Right Path
The Media Monitoring Committee

[131] Source : A Table of Statistics for the Video Relases (s.d.). Repéré à https://ctc.usma.edu/app/uploads/2018/08/A-Table-of-the-Statistics-for-the-video-releases.pdf

ANNEXE 3. The 10 Video Releases for month of Rajab[132]

In the Name of God, the Most Gracious, the Most Merciful

Top 10 Video Releases for the Month of Rajab

Scoring	Name of Release
1	Wilayat Aleppo – Invading Villages to Spread the Guidance
2	Wilayat al-Fallujah – Where to Escape?
3	Wilayat Salahuddin – The Attackers
4	Wilayat al-Raqqa – And Allah will Enrich You from His Blessings
5	Wilayat al-Fallujah – With Hardship will be Ease
6	Wilayat al-Anbar – With Patience and Certainty You will be Granted Victory
7	Wilayat Salahuddin – The Clashing of Swords
8	Wilayat al-Fallujah – And Give Glad Tidings to the Patient Ones
9	Wilayat al-Furat – The Greatest Losers
10	Wilayat al-Khayr – The Sparkle of Sword and Hope

And God is He Who Grant Success and He Guides Us for the Right Path

The Media Monitoring Committee

[132] Source : Top 10 Video Releases for the Month of Rajab (s.d.). Repéré à https://ctc.usma.edu/app/uploads/2018/08/Top-Ten-Releases-Month-of-Rajab.pdf

ANNEXE 4. Liste du matériel

2.1. Documentations de l'État islamique : Liste des documents mis à disposition par le CTC.

A Table of Statistics for the Video Relases (s.d.). Repéré à https://ctc.usma.edu/app/uploads/2018/08/A-Table-of-the-Statistics-for-the-video-releases.pdf.

Clarification Regarding the Media of the Islamic State (s.d.). Repéré à https://ctc.usma.edu/app/uploads/2018/08/Clarification-Regarding-the-Media-of-the-Islamic-State.pdf.

General Guidance and Instructions (s.d.). Repéré à https://ctc.usma.edu/app/uploads/2018/08/General-Guidance-and-Instructions.pdf.

Information Security. Repéré à https://ctc.usma.edu/app/uploads/2018/08/Information-Security.pdf.

Organizational Structure of the Media Office (s.d.). Repéré à https://ctc.usma.edu/app/uploads/2018/08/Organizational-structure-of-the-media-office.pdf.

Responsabilities of Media Offices towards A`maq Agency (s.d.). Repéré à https://ctc.usma.edu/app/uploads/2018/08/Responsibilities-of-Media-Offices-towards-Amaq-Agency.pdf.

Summary Advice for Media Mujahid (s.d.). Repéré à https://ctc.usma.edu/app/uploads/2018/08/Summmary-advices-for-media-mujahid-not-fully-translated.pdf.

The Essential Duties of the Media Mujahid (s.d.). Repéré à https://ctc.usma.edu/app/uploads/2018/08/The-Essential-Duties-of-the-Media-Mujahid.pdf.

The table to Evaluate Video Releases (s.d.). Repéré à https://ctc.usma.edu/app/uploads/2018/08/The-Table-to-Evaluate-Video-Releases.pdf.

Top 10 Video Releases for the Month of Rajab (s.d.). Repéré à https://ctc.usma.edu/app/uploads/2018/08/Top-Ten-Releases-Month-of-Rajab.pdf.

2.2. Documentations des plateformes numériques

2.2.1. Facebook

Facebook (2017, 15 juin). Hard Questions : How We Counter Terrorism. *Facebook Newsroom.* Repéré à https://about.fb.com/news/2017/06/how-we-counter-terrorism/.

Facebook (2017, 26 juin). Facebook, Microsoft, Twitter and YouTube Announce Formation of the Global Internet Forum to Counter Terrorism. *Facebook Newsroom.* Repéré à https://about.fb.com/news/2017/06/global-internet-forum-to-counter-terrorism/.

Facebook (2017, 28 novembre). Are We Winning the War on Terrorism Online ?. *Facebook Newsroom*. Repéré à https://about.fb.com/news/2017/11/hard-questions-are-we-winning-the-war-on-terrorism-online/.

Facebook (2017, 31 juillet). Global Internet Forum to Counter Terrorism to Hold First Meeting in San Francisco. Repéré à https://about.fb.com/news/2017/07/global-internet-forum-to-counter-terrorism-to-hold-first-meeting-in-san-francisco/.

Facebook (2018, 23 avril). Hard Questions : How Effective Is Technology in Keeping Terrorists of Facebook. *Facebook Newsroom*. Repéré à https://about.fb.com/news/2018/04/keeping-terrorists-off-facebook/.

Facebook (2018, 31 juillet). Removing Bad Actors on Facebook. *Facebook Newsroom*. Repéré à https://newsroom.fb.com/news/2018/07/removing-bad-actors-on-facebook/.

Facebook (2018, 17 septembre). Combating Hate and Extremism. *Facebook Newsroom*. Repéré à https://about.fb.com/news/2019/09/combating-hate-and-extremism/.

Facebook (2018, 8 novembre). Hard Questions : What Are We Doing to Stay Ahead of Terrorists ?. *Facebook Newsroom*. Repéré à https://about.fb.com/news/2018/11/staying-ahead-of-terrorists/.

Facebook (s.d.). Standards de la communauté. Repéré à https://www.facebook.com/communitystandards/violence_criminal_behavior [consulté le 17 avril 2019].

Facebook (s.d.), Rapport de transparence Facebook. Repéré à https://transparency.facebook.com/community-standards-enforcement#terrorist-propaganda [consulté pour le trimestre oct. 2018 – déc. 2018].

Zuckerberg, M. (2017, 16 février). Building Global community. Publication Facebook. Repéré à https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634/.

2.2.2. Telegram

Telegram (s.d.). Bot API. *Telegram APIs*. Repéré à https://core.telegram.org/bots [consulté le 14 mai 2019].

Telegram (s.d.). Telegram FAQ. Repéré à https://telegram.org/faq [consulté le 14 mai 2019].

2.2.3. Twitter

Twitter (2016, 5 février). Combating Violent Extremism. *Twitter Blog*. https://blog.twitter.com/en_us/a/2016/combating-violent-extremism.html.

Twitter (2016, 18 août). Dernières nouvelles concernant les efforts de Twitter dans la lutte contre l'extrémisme violent. *Twitter Blog*. https://blog.twitter.com/fr_fr/a/fr/2016/lutte-contre-extremisme.html.

Twitter (2016, 23 août). The infrastructure behind Twitter : efficiency and optimization. *Engineering*. Repéré à https://blog.twitter.com/engineering/en_us/topics/infrastructure/2016/the-infrastructure-behind-twitter-efficiency-and-optimization.html.

Twitter (2016, 5 décembre). Partnering to help curb the spread of terrorist content online. *Twitter Blog*. Repéré à https://blog.twitter.com/en_us/a/2016/partnering-to-help-curb-the-spread-of-terrorist-content-online.html.

Twitter (2017, 1 mars). Dernières nouveautés en matière de sécurité. *Twitter Blog*. Repéré à https://blog.twitter.com/fr_fr/topics/product/2017/Dernieres-nouveautes-en-matiere-de-securite.html.

Twitter (2017, 9 mai). Using Deep Learning at Scale in Twitter's Timelines. *Engineering*. https://blog.twitter.com/engineering/en_us/topics/insights/2017/using-deep-learning-at-scale-in-twitters-timelines.html.

Twitter (2017, 26 juin). Global Internet Forum to Counter Terrorism. *Twitter Blog*. Repéré à https://blog.twitter.com/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html.

Twitter (2018, 5 avril). Exapanding and building #TwitterTransparency. *Twitter Blog*. Repéré à https://blog.twitter.com/en_us/topics/company/2018/twitter-transparency-report-12.html.

Twitter (2019, 6 juin). Faciliter la compréhension de nos règles. *Twitter Blog*. Repéré à https://blog.twitter.com/fr_fr/topics/company/2019/faciliter-la-comprehension-de-nos-regles.html.

Twitter (2019, mars). Terrorism and aviolent extremism policy. *Help Center*. Repéré à https://help.twitter.com/en/rules-and-policies/violent-groups.

Twitter (2019, mars). Politique en matière de manipulation de la plateforme et de spam. Répéré à https://help.twitter.com/fr/rules-and-policies/platform-manipulation.

Twitter (s.d.). À propos des API Twitter. *Centre d'assistance*. Repéré à https://help.twitter.com/fr/rules-and-policies/twitter-api [consulté le 14 avril 2019].

Twitter (s.d.). Application des règles de Twitter. *Rapport de transparence*. Repéré à https://transparency.twitter.com/fr/twitter-rules-enforcement.html [consulté pour juillet – décembre 2018].

Twitter (s.d.). Comment publier des photos ou des GIF sur Twitter. *Centre d'assistance*. Repéré à https://help.twitter.com/fr/using-twitter/tweeting-gifs-and-pictures.

Twitter (s.d.). FAQ au sujet des tendaces Twitter. *Centre d'assistance*. Repéré à https://help.twitter.com/fr/using-twitter/twitter-trending-faqs [consulté le 12 mai 2019].

Twitter (s.d.). Règles de Twitter. *Centre d'assistance*. Repéré à : //help.twitter.com/fr/rules-and-policies/twitter-rules [consulté le 20 avril 2019].

2.2.4. YouTube

YouTube (2017, 1 août). An update on our commitment to fight terror content online. *Official Blog*. Repéré à https://youtube.googleblog.com/2017/08/an-update-on-our-commitment-to-fight.html.

YouTube (2017, 26 juin). Facebook, Microsoft, Twitter and YouTube Announce Formation of the Global Internet Forum to Counter Terrorism. *Official Blog*. Repéré à https://youtube.googleblog.com/2017/06/facebook-microsoft-twitter-and-youtube.html.

YouTube (2017, 4 décembre). Expanding our work against abuse of our platform. *Official Blog*. Repéré à https://youtube.googleblog.com/2017/12/expanding-our-work-against-abuse-of-our.html.

YouTube (2018, 23 avril). More information, faster removals, more people – an update on what we're doing to enforce YouTube's Community Guildelines. *Official Blog*. Repéré à https://youtube.googleblog.com/2018/04/more-information-faster-removals-more.html.

YouTube (2018, 1 décembre). Faster removals and tackling comments – an update on what we're doing to enforce YouTube's Community Guidelines. *Official Blog*. Repéré à https://youtube.googleblog.com/2018/12/faster-removals-and-tackling-comments.html.

YouTube (s.d.). Application du règlement de la commuanuté YouTube. *Transparence des informations*. Repéré à https://transparencyreport.google.com/youtube-policy/removals?hl=fr.

YouTube (s.d.). Programme YouTube Trusted Flagger. *Aide YouTube*. Repéré à https://support.google.com/youtube/answer/7554338?hl=fr [consulté le 15 mai 2019].

YouTube (s.d.). Règlesment de la communauté. *Politiques et sécurité*. Repéré à https://www.youtube.com/intl/fr-CA/about/policies/#community-guidelines [consulté le 21 avril 2019].

YouTube (s.d.). Signaler un contenu inapproprié. *Aide YouTube*. Repéré à https://support.google.com/youtube/answer/2802027?co=GENIE.Platform%3DAndroid&hl=fr [consulté le 18 avril 2019].

YouTube (s.d.). Suppression de contenu en vertu de la loi NetzDG. *Transparence des informations*. Repéré à https://transparencyreport.google.com/netzdg/overview?hl=fr.

2.3. Sources audiovisuelles

https://www.youtube.com/watch?v=mZaec_mlq9M *Mark Zuckerberg testifies before Congress* (2018, 10 avril).

2.4. Documents législatifs et règlements

Loi du 13 novembre 2014, France. Repéré à https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029754374&categorieLien=id.

Loi Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG), 1 octobre 2017, Allememagne. Repéré à https://germanlawarchive.iuscomp.org/?p=1245.

Règlement du parlement européen et du conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne, texte du 12 septembre 2018. Repéré à https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52018PC0640&from=EN.

Utilisation de l'Internet à des fins terroristes : plan d'actions franco-britannique, 14 juin 2017, France – Grandre Bretagne. Repéré à https://www.20minutes.fr/societe/1865755-20160614-policiers-tues-yvelines-larossi-abballa-ouvert-facebook-live-revendiquer-meurtres.

2.5. Articles de presse

AFP. (2016, 14 juin). Policiers tués dans les Yvelines : Larossi Abballa a ouvert un Facebook Live pour revendiquer les meurtres. *20 minutes*. Repéré à https://www.20minutes.fr/societe/1865755-20160614-policiers-tues-yvelines-larossi-abballa-ouvert-facebook-live-revendiquer-meurtres.

AFP. (2016, 10 août). Rejet d'une plainte accusant Twitter de disséminer le message de l'EI. *La Presse*. Repéré à https://www.lapresse.ca/international/dossiers/le-groupe-etat-islamique/201608/10/01-5009323-rejet-dune-plainte-accusant-twitter-de-disseminer-le-message-de-lei.php.

Audureau, W. & Seelow, S. (2015, 18 mars). Les ratés de la première vague de blocages administratifs de sites jihadistes. *Le Monde*. Repéré à https://www.lemonde.fr/pixels/article/2015/03/18/les-rates-de-la-premiere-vague-de-blocages-administratifs-de-sites-djihadistes_4596149_4408996.html.

Brooking, E.T. & Peggy S. (2015, 21 décembre). Les Anonymous contre l'État islamique. *Slate.* Repéré à http://www.slate.fr/story/110691/anonymous-contre-daech.

Cottee, S. (2015, 8 octobre). The Cyber Activists Who Want to Shut Down ISIS. *The Atlantic.* Repéré à https://www.theatlantic.com/international/archive/2015/10/anonymous-activists-isis-twitter/409312/.

France info (2017, 10 avril). Fusillade de Las Vegas : pourquoi la revendication du groupe État islamique pose question. *France info.* Repéré à https://www.francetvinfo.fr/monde/usa/fusillade-a-las-vegas/fusillade-de-las-vegas-pourquoi-la-revendication-du-groupe-etat-islamique-pose-question_2399902.html.

Halifa-Legran, S. (2015, 9 janvier). France, Allemagne, Grande-Bretagne… Des lois anti-terroristes toujours plus sévères. *Le Nouvel Obs.* Repéré à https://www.nouvelobs.com/charlie-hebdo/20150109.OBS9624/france-allemagne-grande-bretagne-des-loi-anti-terroristes-toujours-plus-severes.html.

Hempel, J. (2016, 1 août). Twitter's Latest Challenge : Deciding Who's a Terrorist. *Wired.* Repéré à https://www.wired.com/2016/01/twitters-latest-challenge-is-deciding-whos-a-terrorist/.

Klonick, K. (2019, 25 avril). Inside The Team at Facebook That Dealt With the Christchurch Shooting. *The New Yorker*. Repéré à https://www.newyorker.com/news/news-desk/inside-the-team-at-facebook-that-dealt-with-the-christchurch-shooting.

Menn, J. & Volz, D. (2016, 25 juin). Exclusive : Google, Facebook Quietly Move toward Automatic Blocking of Extermist Videos. *Reuters*. Repéré à https://www.reuters.com/article/us-internet-extremism-video-exclusive-idUSKCN0ZB00M.

Oltermann, P. (2018, 5 janvier). Though new German law puts tech firms and free speech in spotlight. *The Guardian*. Repéré à https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight.

Smith, L. (2017, 12 juin). Islamic State piggybacks Baaz's social mega-feed. *BBC Monitoring*. Repéré à https://www.bbc.com/news/technology-40246763.

2.6. Ouvrages, documents et sites de référence jihadistes

Abû Hamzah al-Muhâjir (2016). *Les chemins de la victoire*. Traduit par la librairie al-Himmah, État islamique.

Brachman, J., & Kennedy Boudali, L. (2006). The Islamic Project : Visual Motifs in Jihadi Internet Propaganda. *Combating Terrorism Center (CTC)*. Repéré à https://www.files.ethz.ch/isn/19674/Islamic_Imagery_Project.pdf.

Arnett, P. & Bergen, P. (2005). Extrait d'un untretien avec CNN [Ben Laden, 12 main 1997]. Dans G. Keppel et J.-P. Milelli, *Al-Qaïda dans le texte* (p. 58-61). Paris : PUF.

Hegghammer, T. (2005). Introduction. Abdallah Azzam, l'imam du jihad. Dans G. Keppel et J.-P. Milelli, *Al-Qaïda dans le texte* (p. 115-137). Paris : PUF.

Keppel, G., & Milelli, J.-P. (2005). *Al-Qaïda dans le texte*. Paris : PUF.

Jihadologie. Liberation Blog. Site web : http://jihadologie.blogs.liberation.fr/.

Al-Zawahiri (2005). Lettre d'al-Zawahiri à al-Zarqawi. Dans G. Keppel et J.-P. Milelli, *Al-Qaïda dans le texte* (p. 419-450). Paris : PUF.

The Oxford Dictionary of Islam. *Oxford Islamic Studies Online*. Site web : http://www.oxfordislamicstudies.com/Public/book_odi.html.

Sourdel, J., & Sourdel, D. (1996). Dictionnaire historique de l'islam. Paris : PUF.

2.7. Autres documents

CtrlSec (2018, 21 février). About @TwitterSupport consistency and standards when dealing with abuses of ISIS terrorist accounts. [En ligne] repéré à : https://justpaste.it/TWSUPPORT.

Katiba des Narvalos (2018, 10 mars). Communiqué de presse. [En ligne] repéré à : https://justpaste.it/KDN_memorandum_Twitter_2018-03.

Katiba des Narvalos (2018, 10 mars). *Mémorandum attaques Twitter*. [En ligne] repéré à : https://justpaste.it/KDN_memorandum_Twitter_2018-03.

Site web Global Internet Forum to Counter Terrorism (GIFCT) : https://www.gifct.org.