ISD | Powering solutions to extremism, hate and disinformation

CASM technology

Recherche sur les évolutions de l'écosystème en ligne: Telegram, Discord et Odysee

Henry Tuck, Jakob Guhl, Julia Smirnova, Lea Gerster and Oliver Marsh

AVERTISSEMENT : Ce rapport contient des images et des descriptions de publications que les lecteurs risquent de trouver extrêmement choquants. Ils comprennent des appels à la violence, la glorification du terrorisme et la déshumanisation de communautés minoritaires.

À propos de cette publication

Les acteurs malveillants utilisent un éventail de plus en plus large d'espaces pour diffuser des idéologies néfastes, et saper les droits de l'homme et la démocratie en ligne. Il est essentiel de comprendre l'évolution de leurs idées, de leurs réseaux en ligne et de leurs activités, afin de développer une base solide de preuves factuelles permettant de les contrer de manière efficace et proportionnée. Mais la création de cette base de preuves pose un défi aux capacités techniques et humaines, ainsi qu'aux limites juridiques et éthiques de la recherche. Nous craignons que tous ces contraintes ne font que s'accroitre au moment même où les possibilités de propager des contenus nuisibles en ligne augmentent.

Il est donc préoccupant de constater qu'il est de plus en plus difficile de mener des recherches numériques de manière systématique, éthique et légale. Il en résulte une situation demandent des compromis difficiles entre des biens concurrents, y compris le désir de comprendre et d'atténuer les contenus et les comportements préjudiciables en ligne, la préservation de la vie privée, et le respect des textes juridiques. Dans le présent rapport, nous affirmons qu'il n'y a pas lieu d'en arriver là: des solutions existent, et des mesures devraient être prises dès que possible afin d'assurer un avenir dans lequel les chercheurs disposent des outils nécessaires pour surveiller, suivre et analyser les contenus et les comportements préjudiciables de manière systématique, éthique et légale.

Ce rapport présente les résultats de la phase de recherche d'un projet mené par l'Institut pour le dialogue stratégique (ISD) et CASM Technology, et financé par Omidyar Network.

L'objectif du projet était d'identifier et de tester des méthodologies de recherche pour surveiller et analyser les petites plateformes fermées ou peu modérées. Il fournit des exemples appliqués, ainsi que des preuves des contraintes et des dilemmes rencontrés par les chercheurs. Dans trois petites études de cas sur Telegram, Discord et Odysee, respectivement en allemand, anglais et français, nous cherchons à d'appliquer différentes approches méthodologiques pour analyser les plateformes présentant principalement des barrières technologiques, éthiques et juridiques, ou des barrières de fragmentation..

À propos des auteurs

Jakob Guhl est directeur de recherche senior à l'ISD, où il travaille au sein de l'unité de recherche numérique ainsi qu'avec l'ISD Allemagne. Ses recherches portent sur l'extrême droite, l'extrémisme islamiste, les discours de haine, la désinformation et les théories du complot. Jakob a été invité à présenter ses recherches sur la manière de renforcer la prévention contre l'extrémisme de droite et l'antisémitisme auprès du ministre allemand de l'intérieur.

Lea Gerster est analyste à l'ISD et à l'ISD Allemagne. Elle travaille sur une série de projets axés sur la prolifération des idéologies extrémistes et de la désinformation dans les parties anglophones et germanophones d'Internet. Auparavant, Lea a occupé pendant deux ans des fonctions liées à l'extrémisme en ligne au sein de TRD Policy et du Centre sur la radicalisation et le terrorisme.

Elle a également travaillé comme stagiaire pour le ministère suisse des affaires étrangères et comme bénévole dans une ferme de thé japonaise. Elle est co-auteur du rapport de l'ISD *Crise et perte de contrôle : L'extrémisme numérique de langue allemande dans le contexte de la pandémie COVID-19*. Elle est titulaire d'une maîtrise en études sur la guerre du King's College de Londres et d'une licence en histoire, en études japonaises et en sciences politiques.

Julia Smirnova est analyste senior à l'ISD et à l'ISD Allemagne. Ses recherches se concentrent sur la prolifération de la désinformation, les théories du complot, les discours de haine et les idéologies extremistes en ligne. Elle est co-auteur des rapports de l'ISD *Violence numérique et désinformation contre les candidats principaux aux élections féderales allemandes de 2021, Un virus de méfiance : la chaîne publique russe RT DE et la scène allemande des négationnistes du COVID-19*, et *Campagnes de désinformation contre les élections : conclusions en Saxe-Anhalt.*

Avant de rejoindre l'ISD, Julia a entre autres travaillé comme journaliste pour Der Spiegel et Die Zeit. En tant que correspondant à Moscou pour Die Welt, elle faisait des reportages sur la politique russe, l'annexion de la Crimée et la guerre dans l'est de l'Ukraine. Elle est titulaire d'une maîtrise en conflit, sécurité et développement du King's College de Londres.

Oliver Marsh est consultant chez CASM Technology et fondateur de The Data Skills Consultancy, qui soutient le travail à l'intersection des compétences en matière de données et des compétences non techniques. Auparavant, en tant que fonctionnaire, il a contribué à la création de l'unité de réponse rapide à Downing Street et de la capacité d'adéquation des données du Royaume-Uni après le Brexit au sein du DCMS. Il est membre du groupe de réflexion Demos, Policy Fellow de la Royal Academy of Engineering et chercheur associé honoraire du département d'études scientifiques et technologiques de l'UCL.

Henry Tuck est responsable de la politique numérique à l'ISD, où il dirige les travaux sur la réglementation numérique et les réponses des entreprises technologiques au terrorisme, à l'extrémisme, à la haine et à la désinformation en ligne. Henry supervise le travail du Laboratoire de Politique Numérique (DPL) de l'ISD ainsi que le travail consultatif sur les principales propositions de réglementation numérique en Europe, Amérique du Nord et Océanie. Il collabore avec l'unité d'analyse numérique de l'ISD pour traduire les résultats de recherche en recommandations concrètes dans le cadre de la politique numérique.

Remerciements

Ce rapport n'aurait pas été possible sans le soutien financier du réseau Omidyar. Nous tenons à exprimer notre gratitude à Wafa Ben-Hassine, Anamitra Deb et Emma Leiken pour leur vision, leur soutien constant et leurs commentaires perspicaces.

Les auteurs souhaitent également remercier Nestor Prieto Chavana, Jack Pay et Carl Miller de CASM, dont l'expertise technique et les conseils ont été essentiels à cette recherche.

Copyright © ISD (2023). Institute for Strategic Dialogue (ISD) est une société à responsabilité limitée par garantie, siège social à l'adresse PO Box 75769, Londres, SW1P 9ER. ISD est enregistrée en Angleterre sous le numéro d'enregistrement de société 06581421 et sous le numéro d'enregistrement d'organisme de bienfaisance 1141069. En France, l'ISD est établi sous la forme d'une association Loi 1901 : l'Institut pour le Dialogue Stratégique sous le numéro d'enregistrement W751256497. Tous droits réservés. Toute copie, reproduction ou exploitation de tout ou partie de ce document ou de ses pièces jointes sans l'autorisation écrite préalable d'ISD est interdite.

ISD | Powering solutions to extremism and polarisation

Amman I Berlin I London I Paris I Washington DC

www.isdglobal.org

Sommaire

Résumé **5**
Glossaire **9**
Introduction **11**
Étude de cas nº 1 : Telegram **13**
Vue d'ensemble de la plateforme 14
Étude de Telegram 16
Analyse des communautés Telegram : principaux résultats 23
Étude de cas nº 2 : Discord **27**
Vue d'ensemble de la plateforme 28
Étude de Discord 29
Analyse des communautés Discord : principaux résultats 34
Étude de cas nº 3 : Odysee **41**
Vue d'ensemble de la plateforme 42
Étude d'Odysee 44
Analyse des communautés Odysee : principaux résultats 46
Conclusions et recommandations **54**
Implications pour les chercheurs 54
Contexte réglementaire 55
Recommandations 60
Endnotes **64**

Résumé

Les acteurs nuisibles utilisent un éventail toujours plus large d'espaces numériques en ligne afin de propager des idéologies préjudiciables et porter atteinte aux droits de l'homme et à la démocratie. Il est essentiel de comprendre l'évolution de leurs idées, de leurs réseaux en ligne et de leurs activités afin de développer une base de données exhaustive, ce qui permettra de déployer des efforts efficaces et proportionnés pour les contrer. Cependant, la création de cette base de données risque de mettre à l'épreuve les capacités techniques, les ressources et même les limites éthiques ainsi que le cadre légal de la recherche. Nous redoutons que ces problèmes s'aggravent, alors que les possibilités de nuire en ligne augmentent.

Cette difficulté à mener des recherches numériques de manière systématique, éthique et légale aboutit à une situation dans laquelle des arbitrages doivent être faits entre des priorités concurrentes, notamment le désir de comprendre et d'atténuer les contenus et les comportements préjudiciables en ligne, la préservation de la vie privée et le respect des accords juridiques. Dans ce rapport, nous soutenons qu'il ne doit pas en être ainsi : des solutions existent, et il faut agir dès que possible afin de garantir un cadre à l'épreuve du temps, dans lequel les chercheurs disposeraient des outils nécessaires pour surveiller, suivre et analyser les contenus et comportements préjudiciables de manière systématique, éthique et légale.

Ce rapport, financé par Omidyar Network, présente les résultats de la phase de recherche d'un projet mené par l'Institut pour le dialogue stratégique (ISD) et CASM Technology. L'objectif du projet est d'identifier et de tester des méthodologies de recherche pour le suivi et l'analyse de petites plateformes fermées ou peu modérées. Le rapport fournit des exemples concrets ainsi que des preuves des limites et des difficultés rencontrées par les chercheurs. À travers trois courtes études de cas portant sur Telegram, Discord et Odysee (respectivement en allemand, en anglais et en français), nous cherchons à appliquer différentes approches méthodologiques afin d'analyser des plateformes qui présentent essentiellement des obstacles d'ordres technologique, éthique et juridique ou liés à la fragmentation.

Obstacles à la recherche (principaux résultats)

- **D'une façon générale, il est possible mais difficile de mener des recherches numériques d'une façon à la fois systématique, éthique et légale sur des plateformes telles que Telegram, Discord et Odysee.** Des considérations éthiques se rapportant au droit à la vie privée ou aux attentes en matière de respect de la vie privée nous ont empêchés de mener des recherches sur des communautés Telegram plus nuisibles, tandis que des préoccupations d'ordre juridique relatives à la violation du droit des contrats nous ont empêchés de collecter systématiquement des données sur les serveurs de Discord. Par conséquent, des barrières éthiques et juridiques limitent la capacité des chercheurs à étudier de manière systématique les communautés nuisibles sur ces plateformes. Bien que l'étude d'Odysee ait engendré moins de problèmes éthiques en raison de sa nature publique, la combinaison de sa complexité technique et le manque de clarté de ses conditions d'utilisation (Terms of Service ou TOS) concernant la collecte des données ont également rendu son analyse complète plus difficile.
- **Sur Telegram, les fonctionnalités de la plateforme permettent aux administrateurs d'espaces que l'on peut penser être publics d'empêcher la recherche systématique de communautés nuisibles.** Telegram permet aux usagers de créer des canaux et des groupes « privés » qui ne peuvent pas être systématiquement trouvés ni étudiés. Comme ces canaux peuvent compter des milliers de membres, ils mettent à l'épreuve la définition du terme « privé ». Les chercheurs qui rejoignent ces canaux peuvent être amenés à dissimuler leur identité, ce qui induit des problèmes d'ordre éthique.
- **Sur Discord, la fragmentation, les obstacles d'ordres éthique et juridique se sont combinés pour limiter la portée des résultats de nos recherches.** L'interface de programmation d'applications (API) de Discord et les fonctions de recherche non transparentes fournies par la plateforme, ainsi que d'autres logiciels tiers présentent des obstacles à la fragmentation. Dans le même temps, les conditions d'utilisation de Discord interdisent la collecte des données utilisateur via son interface de programmation, ce qui peut engendrer des risques d'ordre juridique pour les chercheurs. Par ailleurs, les questionnaires permettant de rejoindre les groupes exigeaient de devoir mentir d'une façon conséquente ou de promouvoir des croyances problématiques, ce qui nous a empêchés de rejoindre de nombreux serveurs intéressants.

- **La conception d'Odysee basée sur la blockchain (un obstacle technologique) a présenté moins d'obstacles insurmontables à la recherche que ce à quoi nous pouvions nous attendre.** Les transactions utilisant la cryptomonnaie LBC sont de fait publiquement visibles et fournissent des données supplémentaires. Cependant, l'étude et la combinaison de différents outils requièrent une expertise technique et un effort substantiels : de nombreuses organisations peuvent ne pas avoir accès à une telle expertise et moins d'outils à code source ouvert peuvent être disponibles en raison du caractère nouveau de la blockchain. La nature audiovisuelle de la plateforme a posé d'autres défis, les chercheurs ayant dû inspecter les contenus manuellement. Les conditions d'utilisation floues sur Odysee ont également conduit à des incertitudes sur ce qui pouvait être approprié ou acceptable d'un point de vue légal.
- **Les obstacles d'ordres technologique, éthique et juridique ainsi que les obstacles liés à la fragmentation sur Telegram, Discord et Odysee sont donc fortement liés les uns aux autres.** Des considérations juridiques nous ont par exemple empêchés de surmonter les obstacles liés à la fragmentation par des méthodes de recherche systématiques sur Discord. De même, des caractéristiques technologiques sur Telegram ont créé des obstacles d'ordre éthique.

Implications pour les chercheurs (principaux résultats)

Les recherches menées dans le cadre de ce projet ont démontré la manière dont les plateformes pouvaient délibérément ou par inadvertance limiter la recherche d'intérêt public de différentes manières.

- **Les choix d'ordre technologique des plateformes peuvent empêcher l'accès aux données ou aux contenus hébergés mais également rendre la collecte de données inutilement fastidieuse d'un point de vue technique**, par exemple lorsque leurs architectures front-end (côté interface) ou back-end (côté serveur) sont fragmentées ou mal entretenues, ou que les outils disponibles pour accéder aux données sont mal documentés. Tous les chercheurs ne disposent pas de l'expertise requise pour pouvoir explorer les possibilités techniques d'un éventail de différentes plateformes, en particulier dans la société civile.
- **Le manque de clarté des conditions légales des plateformes peut engendrer des charges ou des risques supplémentaires pour les chercheurs, augmentant ainsi le coût et les obstacles pour accéder à la recherche en ligne**. Nous avons eu la chance de pouvoir bénéficier d'une aide juridique externe et pro bono, ce qui nous a permis d'évaluer avec plus d'attention les conditions d'utilisation des plateformes et les risques juridiques liés à l'accès aux données.
- **Les plateformes peuvent délibérément invoquer des préoccupations d'ordres juridique ou éthique pour justifier les restrictions d'accès aux données par les chercheurs**, notamment autour de la protection des données ou du droit à la vie privée des utilisateurs. Cela peut se produire même lorsque les utilisateurs ont activement consenti au partage et à l'usage de leurs données à des fins de recherche spécifiques et limitées, ou lorsque la désignation d'espaces en ligne comme privés risque de créer une incertitude d'ordre éthique même si, dans la pratique, ces espaces sont facilement et largement accessibles aux utilisateurs comme aux chercheurs.
- **Il existe un danger pour les maigres ressources de la communauté de chercheurs destinées à répondre à ces difficultés que celles-ci soient employées d'une manière déconnectée et cloisonnée**. Par conséquent, en l'absence de mécanismes et d'incitations fortes en faveur d'une meilleure collaboration, l'on perd l'opportunité de réaliser de grandes économies d'échelle.
- **Des obstacles à la recherche en ligne peuvent créer un ensemble d'incitations problématiques pour les chercheurs** lorsqu'il s'agit d'équilibrer ou de modérer les différents risques d'ordres juridique ou éthique. La tromperie peut par exemple servir à réduire le risque juridique pour les chercheurs utilisant des outils de recherche tiers qui contreviennent aux conditions d'utilisation des plateformes : si les plateformes ou les utilisateurs ne sont pas conscients du fait qu'une collecte de données a lieu, alors la probabilité que les chercheurs soient confrontés à des poursuites judiciaires est considérablement réduite.

- **L'utilisation d'outils tiers ou de méthodes trompeuses peut dissuader les chercheurs à publier leurs travaux et/ou les inciter à rester dans le flou quant à leurs méthodologies de recherche**. Cela a à son tour un impact négatif sur la qualité, la comparabilité et le caractère reproductible de la recherche en ligne sur les questions sociétales et peut engendrer davantage de méfiance entre les plateformes et la communauté de la recherche au sens large.

Communautés extrémistes sur Telegram, Discord et Odysee (principaux résultats)

- **Sur Telegram, les chercheurs de l'ISD ont identifié six canaux privés de langue allemande et 80 groupes privés associés à l'extrémisme d'extrême droite et à des théories conspirationnistes nuisibles, avec 12 049 abonnés pour le plus grand de ces canaux**. Nos résultats suggèrent que même ces espaces plus grands, prétendument privés, sont utilisés à des fins préjudiciables, notamment pour appeler à la violence contre des politiciens, diffuser de fausses informations et pour coordonner la mobilisation sur le terrain.
- **Sur Discord, les chercheurs d'ISD ont identifié 31 serveurs catholiques extrémistes de langue anglaise comptant au total 9 585 abonnés et 16 serveurs extrémistes islamistes avec un total de 4 757 abonnés**. Sur ces serveurs, nos recherches ont mis à jour des quantités significatives de contenus extrêmement haineux, ciblant la communauté LGBT, les personnes de confession juive et les femmes. Les extrémistes catholiques comme islamistes y expriment des opinions antidémocratiques, appellent à l'instauration d'États totalitaires religieux et partagent des contenus violents, notamment en soutien au terrorisme et aux organisations terroristes.
- **Sur Odysee, les chercheurs d'ISD ont identifié 8 690 vidéos d'extrême droite royaliste de langue française, 6 035 vidéos néo-fascistes et 4 084 vidéos catholiques fondamentalistes**. L'analyse de ces vidéos révèle la présence d'idéologies gravement antidémocratiques au sein des communautés francophones sur Odysee. Il s'agit entre autres de contenus négationnistes et vénérant le national-socialisme, qui constituent tous deux des infractions pénales en France.

Recommandations

Sur la base des résultats, des implications pour les chercheurs et du contexte réglementaire plus large exposés dans le présent rapport, nous avons formulé une série de recommandations à l'intention de toutes les plateformes en ligne, des décideurs politiques et des régulateurs ainsi que des chercheurs universitaires et de la société civile afin qu'ils puissent dégager des solutions à l'éventail d'obstacles d'ordres technologique, éthique, juridique et liés à la fragmentation que nous avons rencontrés durant nos recherches.

Nous reconnaissons que certaines de nos recommandations entraîneront un surcroît de travail pour les plateformes, notamment pour les plus petites qui disposent de moins de ressources et de capacités techniques. Toutefois, à l'heure actuelle, les plateformes proposent des fonctionnalités efficaces pour faciliter la communication et la coordination des acteurs nuisibles et n'offrent que des fonctionnalités réduites ou médiocres pour les recherches d'intérêt public dans ces espaces. Nous estimons qu'il faut remédier à ce déséquilibre.

Obstacles d'ordre technologique

- Les plateformes devraient fournir un accès autorisé aux données (via leurs API par exemple) aux chercheurs tiers menant des travaux de recherche d'intérêt public. À cela devrait s'ajouter une documentation claire, cohérente et accessible, comprenant des conseils sur les types de données pouvant être collectées et des limites suffisantes à la collecte de données personnelles sensibles pour protéger la vie privée des utilisateurs.
- Dans le cadre des réglementations futures, les décideurs politiques et les régulateurs devraient exiger de toutes les plateformes un accès aux données qui soit précis, fiable et suffisant pour les travaux de recherche d'intérêt public. Cela inclurait l'éventail plus large des plateformes en ligne de petite et de moyenne taille et ne se concentrerait pas seulement sur les plus grandes, comme c'est le cas actuellement.

- Les chercheurs universitaires et de la société civile devraient partager leurs méthodes ou leurs outils de collecte de données efficaces ainsi que toutes leurs connaissances afin de pouvoir suivre le rythme de la multiplication des plateformes en ligne au sein d'un écosystème en ligne en constante évolution.

Obstacles liés à la fragmentation

- Les plateformes devraient fournir un accès à leurs données d'une manière systématique qui permette aux chercheurs un accès fiable à des données précises provenant de l'ensemble de leurs espaces publics, plutôt que de les contraindre à identifier manuellement les espaces en ligne ou les communautés d'intérêts. Les outils pour la recherche systématique, qu'ils soient propres aux plateformes ou tiers, devraient faire preuve de leur fiabilité, de leur couverture et de leur précision, par le biais d'un avis émis par une tierce partie par exemple.

Obstacles d'ordre éthique

- Les plateformes devraient déterminer une limite raisonnable pour le nombre de membres pouvant participer à des groupes ou à des canaux et déclarer publics les espaces en ligne dont le nombre de membres dépasserait un certain seuil. Les contenus pour lesquels il n'existe pas d'attentes raisonnables en matière de respect de la vie privée (les contenus postés par exemple sur des pages publiques) devraient être rendus disponibles par l'intermédiaire d'un accès contrôlé à l'API.

- Si les plateformes étaient réticentes ou peu enclines à le faire volontairement, les décideurs politiques pourraient envisager d'exiger des entreprises qu'elles clarifient quels espaces de leurs plateformes sont véritablement publics ou privés et qu'elles établissent des seuils raisonnables quant au nombre d'utilisateurs pouvant participer à des espaces en ligne privés.
- La communauté des chercheurs devrait travailler à formaliser une approche éthique en matière de recherche en ligne sur les espaces publics, semi-privés et privés, en adéquation avec la gravité potentielle des risques que ces espaces pourraient poser, tout en respectant le droit à la vie privée des utilisateurs.

Obstacles d'ordre juridique

- Les plateformes devraient fournir des conditions d'utilisation claires, non seulement en ce qui concerne les types de contenus et d'activités qu'elles autorisent, mais aussi sur la façon dont elles s'appliquent aux chercheurs accédant aux données. Ces conditions devraient être ensuite appliquées de manière cohérente.
- Les décideurs politiques devraient mettre en place des protections juridiques pour les chercheurs conduisant des travaux de recherche en ligne d'intérêt public et respectueux de la vie privée.
- Les chercheurs universitaires et de la société civile devraient envisager les possibilités de partager ou de mettre en commun leur expertise sur les implications juridiques de l'accès aux données des plateformes.

Glossaire

Le terme d'**Alt-tech**, pour « technologies alternatives », décrit les plateformes de réseaux sociaux utilisées par des groupes et des individus qui considèrent que les principales plateformes de réseaux sociaux leur sont devenues inhospitalières en raison de leurs opinions politiques. Il s'agit notamment de plateformes construites à des fins politiques spécifiques, de plateformes libertaires qui tolèrent un large éventail de positions politiques, y compris les positions haineuses et extrémistes, et de plateformes non politiques conçues à de tout autres fins, telles que les jeux en ligne.

Une **interface de programmation d'applications (API)** représente l'intermédiaire qui permet à deux applications de communiquer l'une avec l'autre. Leur éventail d'utilisations est très large. Dans le contexte de ce rapport, le terme se rapporte aux API qui permettent aux chercheurs d'accéder à certaines données sur certaines plateformes en ligne via des requêtes. En tant qu'intermédiaire, les API offrent également une protection supplémentaire car elles n'autorisent pas l'accès direct aux données et enregistrent, gèrent et contrôlent les volumes et la fréquence des requêtes.

Les **théories du complot** tentent d'expliquer un phénomène en invoquant une conspiration malveillante orchestrée par des agents puissants. Les complots sont présentés comme secrets ou ésotériques, et les adeptes de la théorie concernée se considèrent comme des initiés qui ont accès à un savoir caché. Les partisans des théories du complot se considèrent généralement comme des opposants directs aux puissances qui tirent les ficelles du complot, celles-ci étant généralement des gouvernements ou des entités faisant autorité.

Les **méthodes d'enquête et de crowdsourcing** (« participation des internautes ») impliquent que les utilisateurs de plateformes en ligne signalent volontairement des formes particulières de contenus aux chercheurs. Les mécanismes de signalement peuvent prendre diverses formes, comme des plug-ins ou des formulaires de signalement pour les utilisateurs.

L'ISD définit la **désinformation** comme un contenu faux ou trompeur diffusé dans l'intention de tromper le public ou d'en tirer des profits économiques et/ou politiques, et qui peut porter préjudice à la collectivité. Lorsqu'un contenu de ce genre est diffusé involontairement, nous utilisons le terme de **mésinformation**.

Le **cryptage** se rapporte au processus d'encodage des informations de manière à les rendre incompréhensibles à toute personne extérieure.

Les **méthodes de recherche ethnographique** impliquent un engagement fort et soutenu dans une communauté. Au lieu de s'appuyer sur des technologies de collecte de données, les chercheurs peuvent choisir une approche plus humaine en rejoignant des espaces en ligne, en y participant et en les observant comme des formes de communautés.

L'ISD définit **l'extrémisme** comme la défense d'un système de croyances qui prône la supériorité et la domination d'un groupe d'appartenance identitaire sur tous ceux qui ne font pas partie de ce groupe. Ce système promeut une vision déshumanisante et « altérisante », incompatible avec les valeurs pluralistes et les droits universels de la personne.

Selon notre définition, les **plateformes fragmentées** sont des plateformes dont le contenu en ligne est théoriquement accessible, sans obstacles technologiques ou éthiques, mais sur lesquelles il n'est toutefois pas possible d'effectuer une recherche rapide ou systématique, par exemple au moyen d'une API. Les contenus pertinents doivent donc être trouvés manuellement parmi de grandes quantités d'autres données.

Nous utilisons le terme de **contenus et comportements préjudiciables** pour désigner un large éventail d'activités en ligne susceptibles de porter atteinte aux droits humains, à la société et/ou à la démocratie. Ils peuvent aller du harcèlement ciblé d'individus à l'incitation à la violence contre un groupe particulier, en passant par la diffusion d'éléments de désinformation et de dangereuses théories du complot. Dans certains cas, le risque de préjudice peut être intrinsèque au contenu même, les risques étant accrus avec sa propagation. Dans d'autres cas, le risque de préjudice peut provenir de modèles de comportements dans leur ensemble plutôt que de la nature du contenu en lui-même. Selon les contextes géographiques et juridiques, certaines formes de contenus ou de comportements

préjudiciables peuvent être illégales ou non. Selon la plateforme, les contenus ou comportements préjudiciables peuvent également être couverts ou non par des sortes de « règles communautaires », des normes ou des règles propres à l'entreprise.

Par **haine**, nous comprenons les croyances ou pratiques qui attaquent, diffament ou excluent une catégorie entière de personnes ou nient sa légitimité sur la base de caractéristiques en vertu desquelles elles sont protégées, notamment l'origine ethnique, la religion, le sexe, l'orientation sexuelle ou le handicap. Les acteurs haineux sont des individus, des groupes ou des communautés qui s'investissent activement et ouvertement dans les activités ci-dessus, ou des individus qui attaquent implicitement des catégories de personnes, par exemple en recourant à des théories du complot et à la désinformation. Les activités haineuses sont considérées comme contraires au pluralisme et à l'application universelle des droits humains.

Les **plateformes ouvertes** sont des plateformes de réseaux sociaux dont le contenu est visible pour le grand public sans authentification particulière et, souvent, accessible au moyen de moteurs de recherche. Par opposition, le contenu des **plateformes fermées** n'est pas facilement accessible par les moteurs de recherche et implique souvent une authentification supplémentaire ou une invitation. Les plateformes comportent souvent à la fois des éléments ouverts et des éléments fermés. Par exemple, sur Facebook, il existe des groupes publics (ouverts) et privés (fermés).

Les **méthodes de recherche systématique** consistent à utiliser la technologie pour extraire directement de grandes quantités de données et de métadonnées des plateformes en ligne. Ces données peuvent comprendre, par exemple, le contenu d'un texte en ligne, les connexions entre des comptes en ligne, ainsi que les métadonnées, comme les heures ou les localisations géographiques des messages. De nombreuses plateformes de médias sociaux facilitent aussi l'accès aux données en proposant des API qui permettent aux chercheurs d'accéder directement à différentes formes de données sur les plateformes sans avoir à créer leur propre code à partir de zéro. Le développement d'approches basées sur l'intelligence artificielle a également permis de créer des méthodes d'analyse de plus en plus sophistiquées. Par exemple, le traitement du langage naturel (TLN) est de plus en plus utilisé pour détecter les tendances, les sentiments et les entités qui apparaissent dans de grands volumes de texte en ligne.

Introduction

Les acteurs nuisibles utilisent un éventail toujours plus large d'espaces numériques en ligne afin de propager des idéologies préjudiciables et porter atteinte aux droits de l'homme et à la démocratie. Il est essentiel de comprendre l'évolution de leurs idées, de leurs réseaux en ligne et de leurs activités afin de développer une base de données exhaustive, ce qui permettra de déployer des efforts efficaces et proportionnés pour les contrer. Cependant, la création de cette base de données risque de mettre à l'épreuve les capacités techniques, les ressources et même les limites éthiques et juridiques de la recherche. Nous redoutons que ces problèmes ne s'aggravent, alors que les possibilités de nuire en ligne augmentent.

Cette difficulté à mener des recherches numériques de manière systématique, éthique et légale aboutit à une situation dans laquelle des arbitrages doivent être faits entre des priorités concurrentes, notamment le désir de comprendre et d'atténuer les contenus et les comportements préjudiciables en ligne, la préservation de la vie privée et le respect des accords juridiques. Dans ce rapport, nous soutenons qu'il ne doit pas en être ainsi : des solutions existent, et il faut agir dès que possible afin de garantir un cadre à l'épreuve du temps, dans lequel les chercheurs disposeraient des outils nécessaires pour surveiller, suivre et analyser les contenus et comportements préjudiciables de manière systématique, éthique et légale.

Ce rapport, financé par Omidyar Network, présente les résultats de la phase de recherche d'un projet mené par l'Institut pour le dialogue stratégique (ISD) et CASM Technology. L'objectif du projet est d'identifier et de tester des méthodologies de recherche pour le suivi et l'analyse de petites plateformes fermées ou peu modérées. Le rapport de la phase initiale de ce projet présentait les résultats de premiers travaux de cadrage des plateformes et de la méthodologie.[1] L'accent avait été mis sur l'identification des obstacles majeurs posés par ces plateformes à la recherche et à la lutte contre les contenus et les comportements nuisibles, mais aussi sur l'examen des méthodologies et des outils de recherche existants pour surmonter ces obstacles. Ce travail nous a permis de définir trois principales catégories d'obstacles : les obstacles technologiques, les obstacles d'ordres éthique et juridique, et ceux liés à la fragmentation.

- **Des obstacles technologiques** peuvent être posés, par exemple, par le cryptage, le contenu généré par l'IA, la blockchain, des structures de plateformes décentralisées ou des formats de contenu (en particulier audiovisuels).
- **Des obstacles d'ordres éthique et juridique** peuvent découler par exemple des attentes en matière de respect de la vie privée, de restrictions juridiques, de conditions d'utilisation des plateformes qui interdisent les travaux de recherche d'intérêt public et de difficultés à obtenir un consentement éclairé. Dans certains cas, les plateformes peuvent présenter des obstacles éthiques sans obstacles juridiques et inversement.
- **Des obstacles liés à la fragmentation** existent sur les plateformes sur lesquelles les contenus en ligne sont théoriquement accessibles sans obstacles technologiques ni éthiques importants, mais ne peuvent pas être recherchés de façon rapide ou systématique, par exemple au moyen d'une API. Les contenus pertinents doivent donc être trouvés manuellement parmi de grandes quantités d'autres données.

Dans ce rapport, nous avions soutenu que la migration depuis les plateformes de médias sociaux traditionnelles vers des espaces en ligne moins soumis à la modération risquait de rendre la recherche et la lutte contre les activités préjudiciables en ligne plus difficiles. Cet argument était basé sur l'observation du fait que nombre de ces plateformes présentaient pour les chercheurs des obstacles d'ordres technologique, éthique et juridique ou liés à la fragmentation, limitant ainsi leurs possibilités d'étudier les communautés nuisibles de manière systématique.

La deuxième phase de ce rapport s'appuie sur cette analyse. Nous y présentons des exemples concrets ainsi que des preuves des limites et des difficultés rencontrées par les chercheurs. À travers trois courtes études de cas, nous cherchons à appliquer différentes approches méthodologiques afin d'analyser des plateformes qui présentent essentiellement des obstacles d'ordres technologique, éthique, juridique ou liés à la fragmentation. Nous avons examiné des communautés en ligne sur Telegram, Discord et Odysee, en langue allemande, anglaise et française respectivement. L'objectif de cet exercice était d'élargir la compréhension du domaine de la recherche quant aux méthodologies applicables à ces espaces en ligne et de fournir des exemples concrets de types d'obstacles auxquels les chercheurs risquaient d'être confrontés en tentant d'accéder à des données sur les plateformes en ligne.

Comme nous le verrons à travers ces études de cas, ces obstacles se chevauchent souvent ou sont liés les uns aux autres, se combinant de différentes façons sur les différentes plateformes. Par exemple, des considérations d'ordre juridique peuvent empêcher de surmonter les obstacles liés à la fragmentation par des méthodes de recherche systématiques. Des caractéristiques techniques peuvent également créer des barrières d'ordre éthique, et des conditions d'utilisation floues ou l'absence d'une API peuvent aussi conduire à des incertitudes autour de ce qui est faisable techniquement ou acceptable d'un point de vue légal. Nous avons choisi de nous concentrer sur trois plateformes.

Les leçons tirées de cette recherche alimenteront la troisième phase du projet, qui visera à apporter des solutions pratiques, techniques et normatives à l'accès aux données et à la transparence pour ces types d'espaces en ligne sans empiéter sur les droits des utilisateurs. Nous partagerons et discuterons de nos résultats avec les parties prenantes concernées, y compris les experts en matière de recherche, les décideurs politiques et les régulateurs, mais aussi les représentants des entreprises du secteur des technologies dont le travail a trait à l'accès aux données et à la transparence. Sur la base de nos résultats, nous nous interrogerons également sur les possibilités d'adaptation du paysage juridique et réglementaire afin que celui-ci puisse suivre le rythme de la multiplication des plateformes en ligne et gérer leur diversité technologique tout en respectant et en protégeant les droits fondamentaux à la vie privée, à la sécurité et à l'anonymat en ligne.

En effet, négocier sur la manière de protéger le droit à la vie privée tout en menant des recherches d'intérêt public sur les communautés et les comportements préjudiciables s'est avéré être l'un des défis majeurs de ce projet. Les préoccupations d'ordres éthique et juridique concernant les attentes légitimes en matière de vie privée seront soulignées tout au long de ce rapport. Malheureusement, il n'existe pas de définition commune des espaces privés, ce qui rend difficile pour les chercheurs de déterminer quels espaces devraient être traités comme étant privés ou publics. Dans le même temps, cette absence de définition permet aux plateformes de limiter la transparence ainsi que l'accès à des espaces privés qui sont aisément accessibles et que l'on peut penser comme étant publics. Comme nous l'avons déjà souligné, des facteurs tels que la taille, l'objectif, l'accessibilité et la nature des relations entre les utilisateurs d'un canal ou d'une communauté devraient être pris en compte lors de l'évaluation de la nature publique ou privée des espaces.[2] Cette incertitude risque également d'affaiblir les arguments en faveur du chiffrement des espaces et des moyens de communication en ligne véritablement privés.

Ce rapport présente tout d'abord les trois études de cas, en commençant par une introduction sur chaque plateforme et sur leurs principales fonctionnalités, ainsi que sur la manière dont elles ont été exploitées précédemment par des communautés nuisibles en ligne. Il décrit ensuite les idéologies et les communautés en ligne spécifiques que nous avons étudiées sur chaque plateforme ainsi que les raisons pour lesquelles nous les avons sélectionnées. Nous documenterons conséquemment les résultats de chaque étude de cas en mettant l'accent sur les préjudices occasionnés par ces différentes communautés. Nous réfléchirons également à la pérennité et aux limites des méthodologies que nous avions identifiées durant la phase initiale afin de surmonter les obstacles que nous avions anticipés mais aussi les obstacles supplémentaires ou inattendus que nous avons rencontrés durant le travail de recherche en lui-même. Cette réflexion inclut une discussion sur les méthodes techniquement faisables mais qui n'ont pas été poursuivies pour des raisons d'ordres éthique, juridique ou liées à des questions de sécurité. Nous nous pencherons dans la dernière section sur la question de savoir dans quelle mesure les trois types d'obstacles et les méthodes de recherche développées durant la phase initiale sont toujours d'actualité ainsi que sur leurs conséquences en matière de collecte de données, d'efforts de recherche et de lutte contre les contenus et comportements préjudiciables sur ces plateformes dans le futur, en mettant particulièrement l'accent sur les conséquences en matière de législation et de politiques numériques.

Étude de cas n° 1 : **Telegram**

Principaux résultats

- Telegram permet aux utilisateurs de créer des groupes et des canaux privés. Leurs contenus ne peuvent faire l'objet de recherches systématiques, car ils présentent des obstacles liés à la fragmentation. Ces espaces étant désignés comme privés, les chercheurs pouvant être ainsi amenés à devoir camoufler leur identité pour les rejoindre, ils présentent également des obstacles d'ordre éthique.
- Néanmoins, ces groupes peuvent compter des milliers de membres, mettant ainsi à l'épreuve la notion d'espace en ligne privé. Il existe aussi des preuves de leur utilisation à des fins préjudiciables, notamment pour préparer des actions potentiellement violentes contre des politiciens allemands.
- Pour ces raisons, nous recommandons à Telegram de déclarer comme publics les groupes et les canaux dont le nombre de membres dépasse un certain seuil et qui, par conséquent, sont soumis aux conditions d'utilisation de la plateforme. Nous recommandons aussi à Telegram de modérer ces espaces d'une façon plus proactive et d'accepter les requêtes de retrait liées à des contenus ou des activités illégales en leur sein.

Pour l'étude de cas concernant les communautés germanophones, l'ISD a entrepris des recherches sur les communautés d'extrême droite et complotistes sur Telegram. Alors que les données disponibles provenant de groupes et de canaux désignés comme publics tendent à être relativement complètes, la recherche sur les groupes désignés comme privés par la plateforme rencontre des obstacles d'ordre éthique et liés à la fragmentation. Leur statut d'espace privé est en effet contestable du point de vue de leur nombre de membres et de leurs objectifs. Nous avons donc tenté d'utiliser une analyse quantitative des liens afin d'identifier les groupes et canaux à haut risque désignés comme privés, avant d'entreprendre une approche ethnographique qualitative dans le but d'analyser ces communautés.

Comme de nombreuses autres plateformes de médias sociaux, Telegram ne définit pas de seuil numérique spécial pour ce qui est considéré comme privé. Au lieu de cela, Telegram permet aux administrateurs de groupes et de canaux de déclarer que ceux-ci sont privés, indépendamment de leur taille. Cela entraîne différentes conséquences importantes sur la manière dont la plateforme est utilisée. Par exemple, dans la mesure où les conditions d'utilisation de Telegram ne s'appliquent qu'à des canaux désignés comme publics, cela crée une faille qui permet de contourner les efforts en matière de modération déjà limités de la plateforme. Alors même que Telegram est conscient de ce problème et affirme qu'en matière de « conflits de contenus » les canaux privés avec des liens accessibles au public sont traités comme des canaux publics[3], il n'existe aucune preuve de modération proactive des canaux privés de la part de la plateforme. Les fonctionnalités des canaux privés permettent également aux administrateurs de générer des fonds grâce à des verrous d'accès payant qui limitent l'accès à ces espaces privés.

Les conséquences sont également problématiques pour les chercheurs. Désigner un groupe comme privé permet aux administrateurs de limiter la visibilité de l'historique des messages aux cent derniers messages pour les nouveaux utilisateurs venant de rejoindre un groupe ou un canal et/ou de restreindre la sauvegarde ou le téléchargement des contenus. Bien qu'en tant que membre du groupe ou du canal il soit techniquement possible d'accéder à ces messages par l'intermédiaire de l'API, cela pourrait contrevenir aux conditions d'utilisation de la plateforme mais également augmenter les risques d'ordre éthique. Les administrateurs pourraient également choisir de désactiver l'accès à l'historique des messages et être alertés de la présence de chercheurs en utilisant cette approche, créant ainsi des difficultés supplémentaires lors de l'étude de communautés extrémistes en ligne. Ces obstacles se combinent pour limiter la capacité des chercheurs à déterminer de manière systématique la présence de contenus préjudiciables dans les groupes ou les canaux privés (ce que nous appelons les obstacles liés à la fragmentation), et ce même lorsque leur taille et leurs objectifs suggèrent fortement qu'il est peu probable que les utilisateurs aient des attentes légitimes ou

réalistes en matière de respect de la vie privée. De ce fait, nous avons étudié le contenu et les comportements des groupes et des canaux en utilisant des méthodes ethnographiques qui ne reposent pas sur une collecte de données systématique à grande échelle, comme nous l'avions indiqué dans la phase initiale de notre rapport.

Toutefois, les études ethnographiques des groupes privés sur Telegram se heurtent à des obstacles d'ordre éthique en raison des questions auxquelles il est souvent nécessaire de répondre avant de pouvoir les rejoindre, les nouveaux membres étant par exemple invités à se présenter et parfois à fournir des informations détaillées d'ordre personnel. Ces questions peuvent obliger les chercheurs à recourir à un certain niveau de tromperie, bien que dans une moindre mesure que sur Discord, comme nous le verrons plus tard. Enfin, les administrateurs contrôlent les membres selon leur comportement, et peuvent même ne partager des liens vers des groupes plus clandestins qu'avec les membres qu'ils considèrent comme dignes de confiance. Cela signifie que les chercheurs doivent créer un faux profil, qui se comportera d'une certaine manière pour gagner en crédibilité et accéder à des groupes nuisibles plus restreints. Il en résulte un compromis difficile : plus un groupe privé suscite l'inquiétude depuis l'extérieur, plus il apparaît légitime d'employer des moyens trompeurs pour le rejoindre. D'un autre côté, il devient de plus en plus difficile de justifier l'intensification des mesures trompeuses, en particulier lorsqu'il s'agit de rejoindre des espaces dans lesquels la frontière entre le privé et le public est floue.

Ces obstacles et ces considérations d'ordre éthique nous ont empêchés de rejoindre des groupes ou des canaux de taille plus restreinte qui nous auraient demandé de recourir à des moyens importants de tromperie. Nos résultats se limitent aux grandes communautés, plus faciles d'accès pour les chercheurs. Nos résultats suggèrent qu'en dépit de leur accessibilité relative, même ces grandes communautés sont utilisées à des fins préjudiciables, notamment pour appeler à la violence contre des politiciens, diffuser de fausses informations et pour coordonner la mobilisation sur le terrain.

Les sections suivantes décrivent l'histoire et les fonctionnalités de Telegram, les méthodes de recherche que nous avons explorées et utilisées, les limites que nous avons rencontrées et les résultats de notre analyse.

Vue d'ensemble de la plateforme

Telegram est une application de messagerie dotée de certaines fonctionnalités de réseau social. Selon ses propres statistiques, elle comptait 700 millions d'utilisateurs mensuels actifs en septembre 2022.[4] Cette plateforme a été fondée en 2013 par les hommes d'affaires russes Pavel et Nikolai Durov. Alors que l'objectif initial déclaré par les fondateurs était de permettre une communication sécurisée sans surveillance gouvernementale, la messagerie s'est développée au fil du temps en une plateforme populaire auprès d'un vaste éventail d'acteurs, incluant des dissidents et des activistes dans des contextes non démocratiques ou autoritaires. Les canaux Telegram (des flux chronologiques de messages auxquels d'autres utilisateurs peuvent s'abonner) sont devenus populaires en tant que plateformes médiatiques pour les acteurs souhaitant diffuser leur contenu auprès d'un public nombreux. Les canaux sont variés, des profils les plus traditionnels aux propagandistes d'État ou aux influenceurs conspirationnistes.

Les conditions d'utilisation de Telegram n'interdisent que la diffusion de contenus pornographiques illégaux et la promotion de la violence par des canaux publics ou des bots, de même que le spam et la fraude.[5] Même si la plateforme a supprimé les canaux liés au terrorisme, en collaboration avec les autorités étatiques, elle ne consacre que peu ou pas d'efforts à la modération d'autres activités illégales ou préjudiciables.[6] Cette situation a rendu la plateforme Telegram particulièrement attrayante pour les acteurs extrémistes et haineux bannis des autres plateformes de médias sociaux.[7]

Fonctionnalités principales

Les utilisateurs de Telegram ont la possibilité de créer et de rejoindre des groupes et des canaux publics et privés. Les groupes publics peuvent être trouvés par l'intermédiaire de la fonction de recherche sur Telegram, et tout le monde peut les rejoindre (mais également voir leur contenu sans devoir les rejoindre). Les groupes et les canaux privés ne

peuvent être rejoints qu'au moyen de liens d'invitation créés par les administrateurs ou par l'ajout manuel des nouveaux utilisateurs par les administrateurs. Bien que Telegram définisse qu'un groupe ou un canal est privé lorsque celui-ci ne peut être trouvé au moyen de la fonction de recherche ni rejoint sans lien d'invitation, le véritable degré de confidentialité dépendra dans la pratique des actions et des choix de ses administrateurs.[8] Les administrateurs peuvent par exemple créer différents liens d'invitation avec différentes limitations : pour chaque lien spécifique, ils ont la possibilité de décider si un individu rejoignant le groupe ou le canal a besoin d'une approbation supplémentaire de leur part. Ils peuvent également fixer une limite quant à la durée de validité du lien et/ou au nombre d'utilisateurs pouvant rejoindre le groupe ou le canal au moyen de ce lien. Enfin, l'espace au sein duquel un lien vers un groupe ou un canal privé est publié peut aussi affecter la confidentialité et la difficulté de pouvoir le rejoindre. Les liens vers des groupes privés peuvent être partagés dans des groupes et des canaux qui comptent un nombre élevé de followers ou, alternativement, les administrateurs peuvent décider de partager ces liens uniquement par messages privés ou de ne pas les partager du tout, et d'ajouter de nouveaux membres manuellement en les sélectionnant parmi leurs contacts.

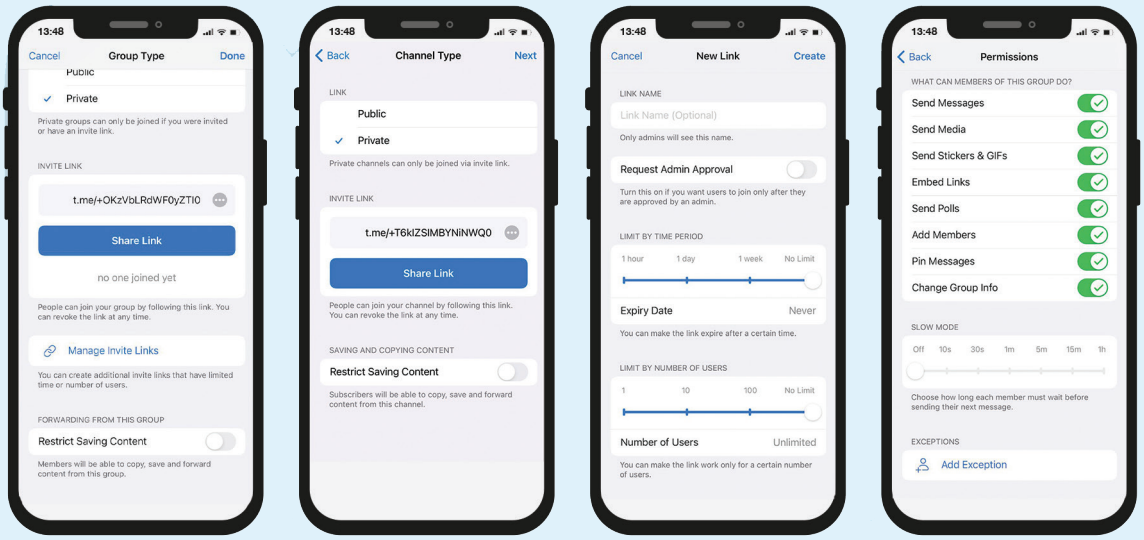


Figure 1: Paramètres administrateur des groupes et canaux Telegram.

Les groupes Telegram privés peuvent compter jusqu'à 200 000 membres. Les grands groupes qui sont privés selon la définition de Telegram peuvent être difficilement considérés comme véritablement privés lorsqu'ils comptent plusieurs milliers de membres susceptibles de tous partager des liens d'invitation dans des espaces publics. TGStat par exemple, un outil russe populaire pour analyser les contenus sur Telegram, contient à la fois des groupes publics et privés dans sa base de données et répertorie régulièrement les canaux privés les plus populaires pour certains pays, en indiquant à la fois leurs noms et leurs liens d'invitation.[9] TGStat collecte des données depuis ces groupes et canaux privés, comme le nombre de participants ou les mentions d'autres groupes ou canaux. Cette pratique a déjà suscité des critiques, en particulier de la part d'utilisateurs en Biélorussie, où les autorités ont arrêté des personnes pour s'être simplement abonnées à des canaux Telegram d'opposition, considérés comme « extrémistes » par le gouvernement.[10] TGStat affirme que les groupes et canaux privés ne se trouvent dans sa base de données que s'ils sont ajoutés par des utilisateurs intéressés par les statistiques ou si des liens vers ces espaces sont partagés fréquemment dans des groupes et canaux publics.[11]

En plus d'offrir des espaces de communication plus ou moins protégés, les paramètres de confidentialité sur Telegram peuvent être utilisés comme un verrou d'accès payant. Par exemple, l'influenceur conspirationniste allemand Oliver Janich[12] possède plusieurs canaux Telegram publics ainsi qu'un canal privé, qui n'est accessible qu'aux abonnés payants.[13] Moyennant un abonnement un peu plus élevé, les utilisateurs peuvent accéder à un chat Telegram privé qui leur permet d'interagir directement avec Janich. Depuis octobre 2022, il est possible de payer les abonnements

au moyen de cryptomonnaies. Janich a été arrêté aux Philippines en août 2022, mais ses différents canaux Telegram continuent de fonctionner, probablement maintenus par son équipe.

Cela signifie que de nombreux groupes considérés comme privés selon la définition de Telegram se trouvent en fait dans une zone grise semblable à celle de certains autres espaces de communication en ligne.[14] Le degré de confidentialité sur Telegram ne dépend pas seulement de fonctionnalités techniques, mais également de la taille des groupes et des décisions de leurs administrateurs. Le tableau ci-dessous montre l'étendue de la confidentialité dans différents types d'espaces sur Telegram.

← Plus public				Plus privé →
Groupes et canaux publics.	Grands groupes privés dont les liens sont publiés sur des canaux publics et sur d'autres plateformes de médias sociaux.	Petits groupes privés dont les liens sont publiés uniquement sur des canaux privés pour une durée limitée. L'approbation des administrateurs peut être requise pour les rejoindre.	Groupes privés dont les liens ne sont jamais publiés sur aucune plateforme de médias sociaux mais plutôt partagés dans des messages individuels privés. Les administrateurs peuvent décider de ne choisir des membres que parmi leurs contacts de confiance.	Messages privés entre deux utilisateurs.

Figure 2: Étendue de la confidentialité pour les groupes ou canaux Telegram.

Activités préjudiciables sur Telegram

Avec peu ou pas d'efforts de modération, Telegram est devenu une plateforme centrale pour les extrémistes internationaux de toutes les idéologies, y compris pour l'extrême droite, les acteurs et les communautés des théories du complot et les opposants au confinement germanophones.[15] Par exemple, en avril 2022, les autorités allemandes avaient annoncé qu'elles avaient déjoué un complot préparé par des acteurs extrémistes connectés via un groupe Telegram visant à kidnapper des personnalités publiques, dont le ministre de la santé.[16] Dans une autre affaire, les autorités avaient ouvert une enquête pénale après qu'une enquête journalistique avait révélé que des membres d'un groupe local d'extrême droite privé sur Telegram à Dresde discutaient de l'assassinat du ministre-président de Saxe (le chef du gouvernement du Land).[17] D'autres enquêtes journalistiques ont documenté de nombreux appels à la violence sur des groupes et des canaux de Telegram.[18] Les enquêteurs fédéraux et régionaux en Allemagne et en Autriche ont également découvert des groupes Telegram dédiés à la vente de drogue, d'armes, de documents falsifiés et de données volées.[19] Alors qu'il existe des preuves évidentes de l'utilisation de Telegram à des fins illégales et préjudiciables, la recherche systématique sur l'étendue et la nature de ces activités au sein de groupes privés fait toujours défaut.

Étude de Telegram

Obstacles d'ordre technologique

D'un point de vue technologique, les données des groupes privés Telegram sont facilement accessibles pour les chercheurs dès qu'ils les ont rejoints. Les membres de groupes fermés peuvent télécharger l'historique des conversations et sauvegarder les listes de leurs membres via l'option « exporter l'historique du chat » dans les paramètres du groupe. Cela permet aussi d'accéder aux textes et aux messages vocaux plus anciens, de même qu'à toute photo, vidéo ou document partagés dans le groupe. Cependant, comme nous l'avons souligné ci-dessus, la désignation d'un groupe comme privé permet aux administrateurs de limiter pour les nouveaux utilisateurs d'un groupe ou d'un canal la visibilité des messages dans l'historique aux cent messages les plus récents. Malgré des tentatives pour se positionner en tant que plateforme axée sur la sécurité et la confidentialité de ses utilisateurs,

Telegram ne propose pas de chats de groupe cryptés de bout en bout. Le cryptage n'est disponible que pour les « chats secrets » entre deux utilisateurs et ne constitue pas une option par défaut mais doit être sélectionné manuellement.

Néanmoins, certaines fonctionnalités de Telegram présentent des défis technologiques pour la recherche systématique. Les messages vocaux et d'autres formes de contenu audiovisuel populaires sur Telegram sont particulièrement difficiles à analyser d'une manière automatisée. De plus, Telegram propose des appels et des vidéos de groupe, impossibles à analyser sans y participer.

Une autre fonctionnalité disponible sur Telegram mais aussi sur de nombreuses autres plateformes et qui représente un défi pour les chercheurs est la messagerie dite éphémère, sur laquelle les messages ne sont visibles que pour une durée limitée. Dans l'un des groupes que nous avons observés, les administrateurs ont activé temporairement la fonction de suppression automatique des messages, rendant ainsi impossible la collecte des messages effacés à l'aide de la fonction d'exportation des chats tout en limitant la durée pendant laquelle les membres du chat pouvaient y accéder. Si ce type de fonctionnalité peut jouer un rôle important dans la protection de la vie privée des utilisateurs, elle représente également un défi de taille pour la recherche en ligne.

Obstacles liés à la fragmentation

Un autre obstacle à la recherche sur Telegram est de trouver des groupes intéressants, en raison de ce que nous avons appelé la fragmentation. Les groupes et canaux privés sont invisibles pour la fonction de recherche de la plateforme et les moteurs de recherche. Il est de ce fait impossible de les trouver grâce à des mots-clés spécifiques. L'une des approches pour les chercheurs consiste à conduire une analyse systématique des liens par l'intermédiaire d'une collecte automatisée dans les groupes et les canaux qu'ils ont déjà rejoints sur Telegram puis de filtrer les liens vers les groupes ou les canaux privés, ou à rechercher des liens dans les bases de données ou sur d'autres plateformes. Les chercheurs pourraient sinon passer manuellement d'un groupe ou d'un canal à l'autre et vérifier, toujours manuellement, si des liens vers d'autres groupes ou canaux y sont postés. Toutefois, ceci est beaucoup plus chronophage que d'utiliser la fonction de recherche. En outre, des liens vers certains groupes clandestins pourraient ne jamais être postés dans les espaces publics et rester par conséquent indisponibles.

Obstacles d'ordre éthique

L'étude des activités préjudiciables en ligne, en particulier celle des communautés extrémistes violentes, pose une série de dilemmes d'ordre éthique que les chercheurs et les universitaires ont déjà examinés en détail, ainsi que les juristes, les gouvernements et les autorités de régulation.[20] Alors même que la compréhension des dynamiques de radicalisation et l'analyse des communications entre les communautés qui fomentent des attaques violentes ou qui sont impliquées dans d'autres activités illégales sont d'intérêt public, les chercheurs peuvent se retrouver dans une position éthique difficile lorsqu'ils doivent trouver un équilibre entre cet intérêt public et les droits des personnes faisant l'objet de leurs recherches.

Ces considérations éthiques constituent une complication majeure lorsqu'il s'agit de rechercher des contenus et des comportements préjudiciables dans des groupes Telegram privés, dans lesquels les utilisateurs s'attendent à communiquer sans intrusion de la part d'observateurs extérieurs. Si les chercheurs veulent obtenir un consentement éclairé afin de respecter pleinement les sujets de leurs recherches et leur confidentialité, ils se doivent d'être transparents quant à leur identité et à leurs objectifs. Ils doivent demander à tous les participants du groupe de consentir à la présence d'un chercheur dans le chat et au stockage potentiel et à l'analyse de leurs données et de leurs messages. Ce consentement est probablement difficile à obtenir, en particulier dans le cas des chats en ligne extrémistes. Sachant qu'ils sont observés, les membres de ces communautés peuvent aussi modifier leur comportement et éviter les contenus potentiellement illégaux ou tout simplement quitter complètement le groupe. Par exemple, les utilisateurs de groupes complotistes qui pourraient considérer que les institutions universitaires et les think tanks font partie d'un complot des élites mondiales seraient peu susceptibles d'accueillir un observateur potentiellement critique. Enfin, il faut considérer les risques encourus par les chercheurs eux-mêmes. Si leur identité

ou l'institution à laquelle ils sont rattachés étaient révélées à des acteurs potentiellement nuisibles, ils risqueraient de devenir la cible d'abus en ligne, de harcèlement, de voir leurs données personnelles être divulguées ou même faire l'objet d'attaques dans le monde réel.

Si les chercheurs estimaient qu'il leur serait soit impossible soit trop risqué de conduire leurs recherches d'une manière totalement transparente, ils pourraient décider que la valeur de l'étude d'un groupe privé particulier l'emporterait sur les problèmes potentiels de confidentialité, d'absence de consentement aux travaux de recherche ou de certaines formes de tromperie. Les chercheurs devraient aussi considérer les coûts de la non-étude des groupes potentiellement violents ou préjudiciables et susceptibles de violer les droits d'autrui ou de préparer des actes violents.

Alors que certains groupes fermés sur Telegram sont aisément accessibles et de facto semi-publics, d'autres ne comptent qu'une poignée de membres et leur accès requiert l'approbation des administrateurs du groupe, qui vont questionner les membres potentiels. Dans le premier cas, les chercheurs peuvent rester des observateurs passifs, sans recourir à aucune méthode de tromperie active. Dans le second cas, ils sont susceptibles d'être interrogés sur leurs motivations à rejoindre le groupe et devront décider s'ils souhaitent fournir de fausses réponses pour obtenir cet accès.

Méthodologie de recherche

Afin de trouver des liens d'invitation à des groupes et des canaux privés, les chercheurs de l'ISD ont rejoint une liste initiale de canaux publics. Cette liste de 253 canaux publics d'extrême droite et complotistes germanophones a été compilée dans le cadre d'un autre projet de l'ISD sur l'extrémisme en Allemagne et mise à jour pour ce projet.[21] Il convient de noter que cette approche n'est possible que pour les chercheurs qui ont accès à des listes à jour de groupes et de canaux existants, celles-ci pouvant être difficiles à créer et à tenir à jour, ce qui représente un obstacle supplémentaire à la recherche.

Les messages publiés par ces canaux du 1er janvier 2022 au 18 août 2022 ont été collectés et les liens ont ensuite été automatiquement extraits de ces messages. Les chercheurs de l'ISD ont vérifié manuellement ces liens vers le domaine t.me de Telegram (un format courant de liens dirigeant directement vers les canaux, groupes et messages sur Telegram) dans le but d'identifier de potentiels liens d'invitation. Sans rejoindre les groupes ou les canaux, il a été possible d'identifier si le lien était actif ou non, de voir le nom du groupe ou du canal privé, ses photos de profil et sa description si elle existait, mais aussi le nombre de membres (groupes) ou d'abonnés (canaux).

Cette analyse a abouti à l'établissement d'une liste de 80 groupes et de 6 canaux privés. Le nombre de membres ou d'abonnés variait entre 8 membres pour le plus petit groupe à 12 049 abonnés pour le plus grand canal.

Alors que certains liens d'invitation issus du jeu initial de données ont été fréquemment partagés, d'autres ne l'ont été qu'une seule fois et n'ont été vus que peu de fois. Le lien d'invitation vers un groupe privé le plus fréquemment partagé était un lien redirigeant vers un canal Telegram complotiste servant d'espace de discussion à ses abonnés : il a été partagé 1 843 fois et vu plus de 35 millions de fois. Ce groupe comptait 2 852 membres, ce qui peut difficilement être considéré comme un espace de communication entièrement privé.

D'un point de vue thématique, d'après les noms et certaines descriptions disponibles, les groupes et canaux du jeu de données initial étaient consacrés aux sujets suivants :

1. Mobilisation en vue de manifestations dans certaines régions et villes d'Allemagne. Si plusieurs groupes indiquaient l'objet de leur manifestation dans la description ou le nom du groupe, d'autres ont utilisé des expressions génériques comme « nous nous soulevons » ou faisaient référence aux « manifestations du lundi », qui étaient initialement une forme de protestation en faveur de la démocratie dans l'ancienne RDA, dont le nom a été repris par les acteurs de l'extrême droite et les covido-sceptiques.

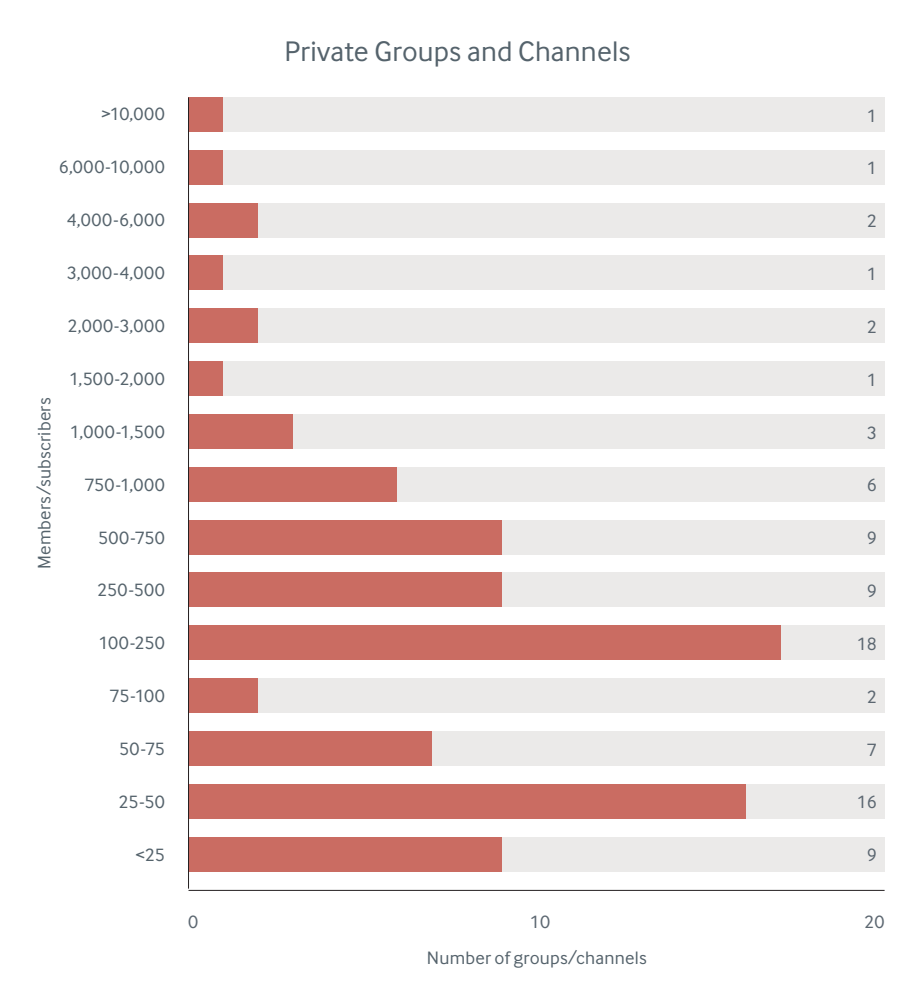


Figure 3: Taille des groupes et des canaux privés dans l'exemple analysé.

2. Discussions sur la pandémie de COVID-19. D'après les descriptions, ces groupes réunissaient des covido-sceptiques et des personnes opposées à la vaccination, bien que certains noms et descriptions étaient plus euphémiques, mentionnant des « libres-penseurs sains » ou la protection des enfants (vraisemblablement contre la vaccination et d'autres mesures contre le COVID-19).
3. Aide locale aux routiers en provenance de Russie. Ces groupes ont été créés après l'invasion de l'Ukraine par la Russie. Les liens d'invitation vers ces groupes étaient partagés largement par les canaux d'extrême droite et complotistes.
4. Événements spécifiques autres que des manifestations, tels que des rassemblements ou des événements ésotériques commerciaux ou des séminaires sur le développement spirituel.
5. Théories du complot, y compris la mouvance QAnon.
6. Sujets ésotériques, comme les médecines alternatives ou le développement spirituel.
7. Réseautage local sans aucune référence au sujet de discussion.
8. Autres sujets ou groupes avec des objectifs peu clairs.

Pour choisir les groupes à rejoindre, nous avons privilégié les groupes ou canaux les plus populaires avec un grand nombre de membres ou d'abonnés, ou ceux qui nous ont semblé les plus extrémistes d'après leurs dénominations ou leurs descriptions, y compris des groupes extrémistes connus ou susceptibles de partager leurs conspirations

préjudiciables. Toutefois, il n'a pas été toujours possible de comprendre correctement les objectifs et le niveau de nuisance potentiel de groupes et canaux sans les rejoindre au préalable. Notre jeu de données contenait par exemple des liens vers un groupe et vers un canal privés partagés par des canaux d'extrême droite et semblant affiliés à un groupe néonazi. En réalité, ces liens étaient liés à un hoax réalisé par des militants antifascistes qui visait à démontrer la manière dont la musique d'extrême droite est diffusée sur les plateformes de streaming musical.[22] Un autre canal privé de notre jeu de données portait un nom trompeur : « la protection animale est une question d'honneur ». Nous avions décidé de nous y abonner, le lien vers ce canal ayant été partagé par le célèbre influenceur allemand conspirationniste et d'extrême droite Attila Hildmann. Il s'est avéré que ce canal était l'un des canaux de réserve de Hildmann pour contourner les restrictions imposées par Telegram sur ses canaux principaux.[23]

Conditions d'entrée

Pour rejoindre et pouvoir publier des messages dans plusieurs groupes de grande taille comprenant plusieurs centaines de membres, les chercheurs ont dû résoudre de simples CAPTCHAS (un test permettant de déterminer si un utilisateur est humain).

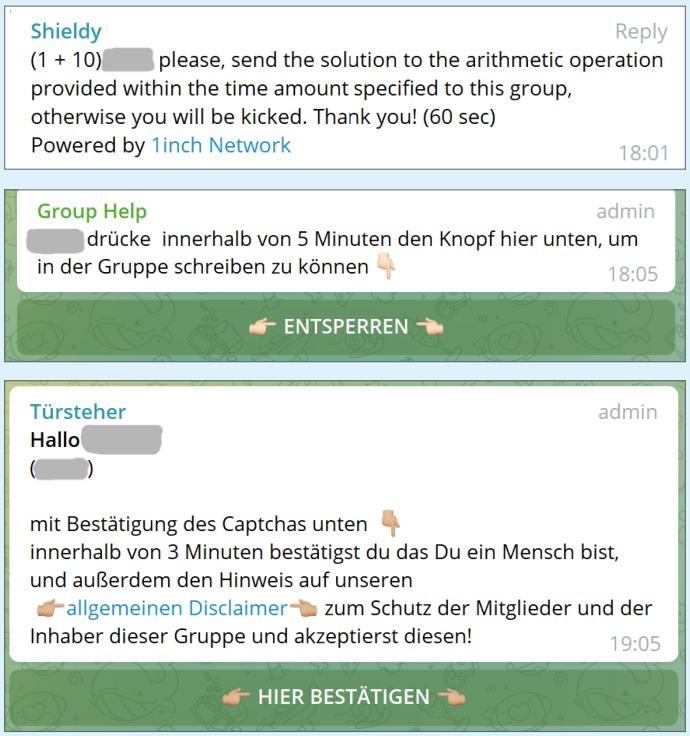


Figure 4: CAPTCHAS dans les groupes Telegram privés.

Dans l'un des groupes comprenant plus de 2 000 membres, un bot demandait aux nouveaux membres de répondre en trois minutes à la question de savoir pourquoi ils rejoignaient le groupe, en optant pour l'une des trois réponses suivantes : 1) « aucune idée » 2) « est-ce important ? » et 3) « je suis curieux ». Ceux qui ont choisi la première ou la seconde option ont été automatiquement exclus du groupe et empêchés de le rejoindre de nouveau.

Dans l'un des petits groupes fermés (un chat local avec pour objectif déclaré de mettre en réseau d'anciens soldats), un bot demandait aux nouveaux membres de se présenter et de fournir quelques informations personnelles. Ces groupes locaux étaient connectés à un canal public Telegram pour les anciens combattants qui comptait plus de 14 000 abonnés. Ce canal a régulièrement publié de la désinformation pro-russe sur la guerre en Ukraine, notamment en provenance de la chaîne d'État russe RT, ainsi que des informations fausses et trompeuses sur la pandémie du COVID-19 et des appels à manifester contre les mesures de santé publique et les sanctions contre la Russie prises par

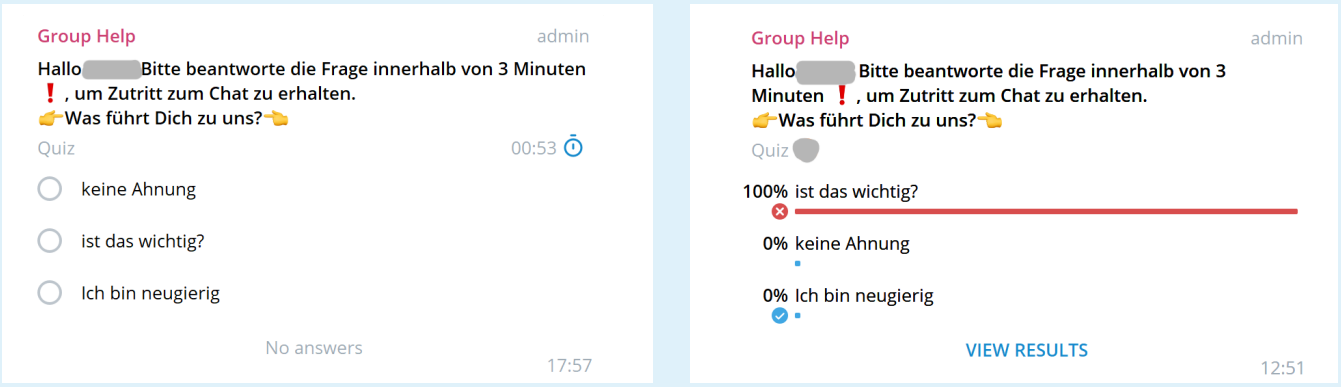


Figure 5: Questions posées par un bot comme barrière pour pouvoir rejoindre un groupe Telegram.

le gouvernement allemand. Le canal était connecté à un groupe public comprenant plus de 600 membres ayant pour fonction de pouvoir commenter le canal.[i] Dans ce groupe public, les membres publiaient des appels à la violence contre les politiciens, appelaient à acheter des armes et à une « insurrection » contre le gouvernement allemand, au lieu de « manifester inutilement ». Il est à noter que les conditions d'utilisation de Telegram n'interdisent pas explicitement la promotion de la violence dans aucun groupe, qu'il soit public ou privé. Selon Telegram, « tous les chats et chats de groupe Telegram sont privés entre leurs participants. Nous ne traitons aucune demande les concernant ».[24]

Figure 6: Appels à la violence et à l'« insurrection » dans un groupe public d'anciens combattants.

Après avoir rejoint le groupe public d'anciens combattants, les chercheurs ont pu voir les liens d'invitation vers les groupes fermés locaux de mise en réseau, qui étaient bien plus petits (de 7 à 100 membres en septembre 2022). La décision de rejoindre de petits groupes fermés tels que ceux-là engendre un dilemme d'ordre éthique. Dans ce cas néanmoins, les chercheurs ont décidé que ces communautés pouvaient potentiellement être nuisibles et dangereuses au regard des appels à la violence dans le chat public et le fait que ces groupes et ces canaux ciblaient des anciens combattants. Les chercheurs ont rejoint l'un des groupes locaux dans lequel les nouveaux membres étaient invités par un bot à se présenter, à nommer les premiers chiffres de leur code postal et à donner des informations sur la durée de leur service dans l'armée. Selon les règles du groupe, les nouveaux membres qui ne se présentaient pas dans les 48 heures étaient exclus du chat. Cependant, dans la pratique, ces règles n'étaient pas appliquées de manière stricte. Les chercheurs ont pu rester dans le groupe alors même qu'ils avaient décidé de ne fournir aucune réponse trompeuse ni d'écrire quoi que ce soit dans le chat.

i Afin de pouvoir commenter des posts sur un canal Telegram, les administrateurs du canal doivent relier celui-ci à un groupe.

Dans l'ensemble, les obstacles à la possibilité de rejoindre de grands groupes dont les liens étaient partagés publiquement étaient relativement faibles. Les chercheurs ont souvent pu rejoindre des groupes et y rester en tant qu'observateurs passifs sans aucune tromperie active. Dans le cadre de cette recherche, nous avons décidé de ne pas rejoindre de petits groupes sans preuves solides de leur implication dans des activités potentiellement violentes. Nous nous sommes aussi abstenus de tout type de tromperie qui aurait pu être nécessaire pour que les récits et les profils des chercheurs soient admis en tant qu'adeptes dans ces communautés, puis invités dans des groupes plus clandestins. Cela signifie que nous n'avons pu analyser que des groupes relativement ouverts.

Analyse des communautés Telegram : principaux résultats

Nous avons dû décider où concentrer notre travail ethnographique parmi les groupes et les canaux privés identifiés par notre analyse de liens. Au regard des preuves d'appels à la violence et d'activités illégales que nous avons trouvées émanant en particulier de groupes d'extrême droite germanophones, anticonfinement et complotistes, nous avons concentré nos recherches sur des groupes extrémistes connus et sur ceux qui appelaient à la violence, à des manifestations sur le terrain et qui étaient susceptibles de planifier des actions violentes. Au total, nos chercheurs ont rejoint 28 groupes et 2 canaux privés.

Au cours de la période d'observation (d'août à septembre 2022), ces groupes ont publié à plusieurs reprises des appels à manifester ou à la « grève générale » contre toutes les mesures encore en vigueur de santé publique relatives au COVID-19, les vaccinations contre le COVID-19, et de plus en plus contre l'augmentation du coût de la vie et les sanctions à l'encontre de la Russie. Les utilisateurs de ces groupes ont souvent transféré des messages en provenance de canaux conspirationnistes ou d'extrême droite, publié des liens vers des médias alternatifs ou d'État russes, tels que RT ou RT DE. Après l'imposition par l'UE de sanctions à l'encontre des médias d'État russes suite à l'invasion générale de l'Ukraine, les utilisateurs des groupes observés ont partagé des conseils sur la manière de contourner les sanctions et ont affiché des liens vers des domaines RT alternatifs. Les membres de ces groupes publiaient également des tracts sur des événements à venir, des photos et des vidéos d'événements se déroulant dans leurs régions comme dans d'autres, probablement pour renforcer le sentiment d'urgence et créer l'impression de manifestations à grande échelle par des personnes partageant les mêmes idées.

Afin de mobiliser les contestataires, les auteurs des publications se sont souvent approprié le langage de la résistance antiautoritaire, affirmant qu'ils manifestaient pour la « liberté », les « droits de l'homme » ou la « paix ». À l'inverse, l'État allemand était dépeint comme une dictature ou un « régime Corona ». Les membres des groupes diffusaient des fausses informations selon lesquelles le gouvernement prévoyait le recours à l'armée contre les manifestants ou de leur tirer dessus. Le gouvernement allemand était aussi dépeint comme étant dirigé par des forces externes ou par une « mafia mondiale de la finance » (un appel du pied antisémite).

Figure 7: Tracts et photos de manifestants partagés dans différents groupes.

Pour l'un des groupes privés, l'ISD a téléchargé tout l'historique du chat afin de tester les possibilités d'une analyse automatisée. Il s'agissait d'un groupuscule émanant d'un groupe local extrémiste, sous observation car soupçonné de « délégitimation anticonstitutionnelle de l'État » par les services de l'Office de protection de la constitution en Saxe-Anhalt (un service national fédéral de renseignement intérieur).[25] Cette nouvelle catégorie a été introduite après les manifestations contre le confinement pour faire face aux acteurs qui délégitimisent et sabotent l'État et les institutions publiques.[26] Après avoir rejoint le groupe, les chercheurs ont pu sauvegarder manuellement l'historique du chat à partir d'une date choisie (dans le cas présent le 1er janvier 2022). Entre le 1er janvier 2022 et le 3 octobre 2022, 767 utilisateurs uniques ont publié 22 165 messages dans le groupe. Le volume de messages a été particulièrement élevé de janvier à mars, la plupart des messages se concentrant alors sur l'opposition aux mesures de santé publique ou sur le début de l'invasion russe générale de l'Ukraine. Le groupe est devenu moins actif en mai et en juin, puis le niveau d'activité a augmenté de nouveau à l'automne, mais pas autant qu'en début d'année.

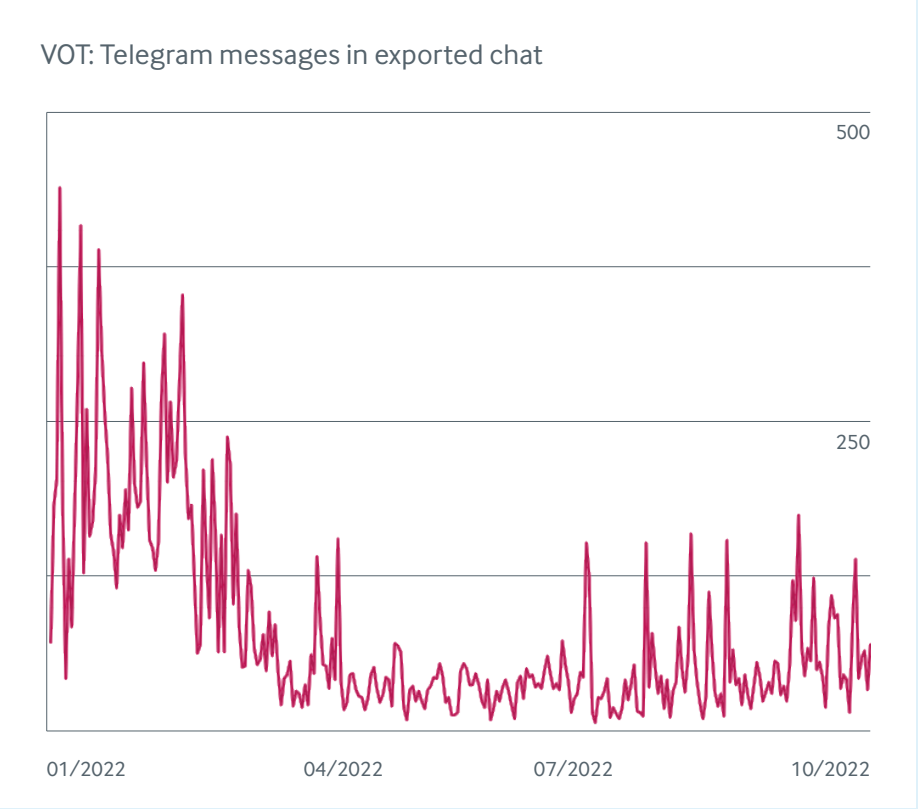


Figure 8: Volume des messages dans le chat exporté du groupe.

La majorité des messages dans le chat a été publiée par un petit groupe d'utilisateurs très actifs. Les 76 utilisateurs les plus actifs (10 % de tous les utilisateurs uniques), définis comme ceux ayant publié 90 messages ou plus, ont été à l'origine de 78,7 % de l'ensemble des messages du groupe. Les trois utilisateurs les plus actifs ont publié chacun plus de mille messages. Par opposition, plus de la moitié des utilisateurs uniques n'ont publié que trois messages ou moins durant la période observée.

Les membres du groupe ont également posté une quantité importante de contenu audiovisuel qu'il a été difficile d'analyser de manière automatisée. Globalement, l'historique du chat, depuis le message le plus ancien publié le 28 avril 2020 jusqu'au 20 octobre 2022, contenait 6 428 images, 3 128 vidéos, 179 messages vocaux, 85 fichiers audio et 603 autres fichiers tels que des PDF ou des fichiers .doc. Le volume des données audiovisuelles a fait de l'analyse approfondie des fichiers de ce seul groupe un défi significatif.

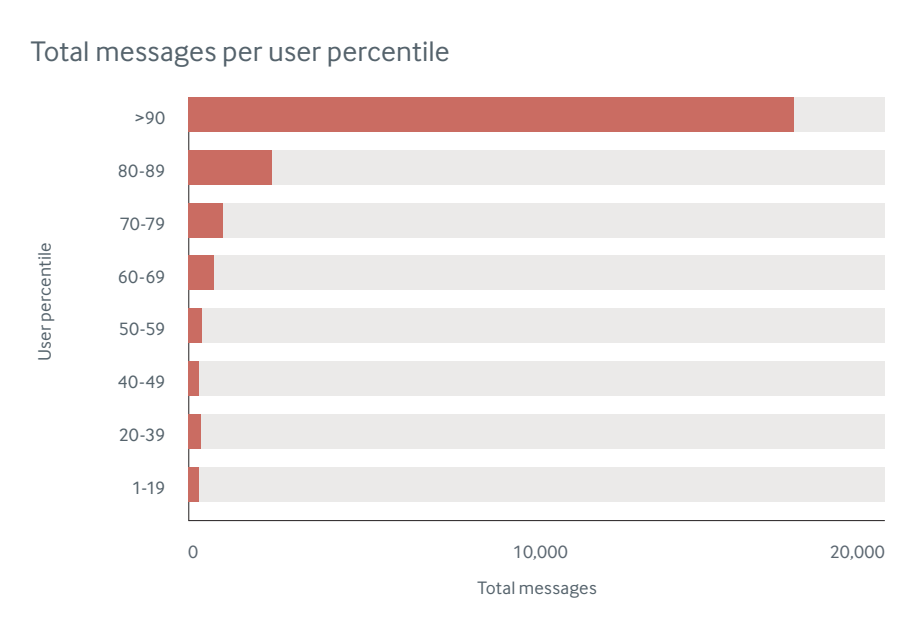


Figure 9: Pourcentage total de messages par utilisateur.

Résultats et recommandations

Telegram reste une plateforme dépourvue de système de modération exhaustif. Même si la plateforme retire sporadiquement du contenu illégal ou faisant l'apologie de la violence, ces actions restent incohérentes et insuffisantes. Les groupes privés offrent des brèches qui permettent de contourner les obligations juridiques de suppression des contenus illégaux mises en place dans des pays comme l'Allemagne. Les contenus publiés dans les groupes privés Telegram ne peuvent pas être détectés de manière automatisée par des moteurs de recherche externes ou par la propre fonction de recherche de Telegram ou son API. Au lieu de cela, les groupes et les canaux doivent être trouvés par une analyse systématique des liens d'invitation, ce qui peut être fastidieux et par conséquent onéreux d'un point de vue des ressources. Cela peut être particulièrement difficile pour les chercheurs ne disposant pas des listes existantes de groupes nuisibles ou qui ne savent pas où les trouver.

Les chercheurs doivent rejoindre des groupes privés pour accéder à leurs contenus, ce qui pose un dilemme d'ordre éthique. Pour accéder aux groupes les plus clandestins et les plus nuisibles, les chercheurs doivent recourir à la tromperie active, c'est-à-dire qu'ils doivent se comporter comme les autres membres du groupe en publiant des messages haineux ou extrêmes, ou payer des abonnements ou effectuer des dons à des acteurs nuisibles afin d'être acceptés comme membres de confiance de la communauté. Alors que ces ruses sont parfois employées par les journalistes[27] ou les forces de l'ordre et les services de renseignement, nous avons décidé de nous abstenir de payer des extrémistes ou de recourir à la tromperie pour des raisons d'ordre éthique.[28]

En raison d'obstacles liés à la fragmentation et d'ordre éthique, nos recherches sur les communautés nuisibles se sont donc limitées à de grands groupes privés dont les liens étaient partagés dans des canaux publics. Nous avons pu constater que certaines de ces grandes communautés mettaient à l'épreuve la définition d'espace en ligne privé en raison de leur taille et du fait que les liens d'invitation étaient activement partagés sur des canaux publics. Même ces espaces semi-publics ont été employés pour des appels à la violence, la diffusion de théories du complot préjudiciables et pour mobiliser sur le terrain.

Le fait que les règles de Telegram ne s'appliquent ni aux groupes publics ou privés (qui peuvent compter jusqu'à 200 000 membres) ni aux canaux privés rend ces espaces en ligne attirants pour les acteurs nuisibles afin de relayer les

appels à la violence et la désinformation, mais aussi pour mobiliser des communautés pour des actions sur le terrain. Pour remédier à ces préjudices, Telegram devrait instaurer une limite raisonnable au nombre de membres pouvant participer à des groupes ou des canaux privés. Les espaces en ligne dont le nombre de membres dépasse un certain seuil devraient être déclarés publics et être ainsi soumis aux conditions d'utilisation de Telegram. Telegram devrait aussi s'engager à faire respecter ses conditions d'utilisation d'une manière plus systématique et efficace afin de limiter le volume de contenus, de comportements et de communautés illégaux ou préjudiciables sur la plateforme. Enfin, Telegram devrait veiller à ce que les chercheurs puissent accéder et obtenir des données sur ces espaces en ligne publics, tout en garantissant à leurs utilisateurs des mesures de protection de leur vie privée et de leurs données.

Étude de cas n° 2 : **Discord**

Principaux résultats

- Discord présente des problèmes similaires à ceux de Telegram. En effet, les chercheurs doivent rejoindre une communauté (ou un serveur) pour accéder à du contenu, ce qui induit une fragmentation qui fait obstacle à la recherche systématique, ainsi que de potentiels problèmes d'ordres éthique et juridique concernant la tromperie et l'utilisation des données.
- Discord est concerné par des problèmes similaires relatifs à la distinction entre groupes publics et privés. De plus, les fonctionnalités de taggage (d'« étiquetage ») et de recherche de Discord, qui permettent aux utilisateurs de trouver les serveurs qui les intéressent, semblent présenter différents problèmes, car ils produisent des résultats incohérents quand on les compare à des solutions alternatives. Les serveurs mélangent souvent les comportements préjudiciables et les comportements sociaux en général, ce qui rend la localisation du matériel pertinent encore plus difficile.
- Toutefois, nous avons pu effectuer une étude (limitée) de deux différentes communautés religieuses extrémistes : catholique et islamiste. Dans ces deux groupes distincts, nous avons constaté des comportements préjudiciables similaires, notamment la haine anti-LGBTQ, l'antisémitisme et les appels à l'établissement d'États religieux fondamentalistes.

Pour l'étude de cas portant sur les communautés en ligne anglophones, l'ISD a analysé celles qui, sur Discord, font la promotion de deux types d'extrémisme religieux : catholique et islamiste. Discord présente principalement des obstacles liés à la fragmentation. Pour contourner ces obstacles, les chercheurs ont adopté deux approches méthodologiques différentes : 1) l'accès systématique aux données limitées aux serveurs d'intérêt spécifique et 2) la recherche ethnographique.

Discord pose des obstacles liés à la fragmentation de deux manières distinctes. Premièrement, s'il est techniquement possible de rechercher et de télécharger des messages via l'API de Discord, cela ne se fait que serveur par serveur, ce qui signifie que les chercheurs doivent savoir où chercher du contenu préjudiciable et être membres des serveurs en question. Deuxièmement, il est encore plus difficile de savoir où chercher des contenus ou des communautés pertinents en raison des limitations des fonctions de recherche non transparentes offertes par la plateforme ou par des logiciels tiers.

Si les obstacles liés à la fragmentation sont les principaux obstacles sur Discord, la plateforme présente également des obstacles d'ordres juridique et éthique distincts. Les conditions générales d'utilisation de Discord interdisant la collecte de données utilisateur via son API, la collecte de données de cette manière à partir des serveurs semblerait enfreindre le droit des contrats et risquerait d'entraîner une action en justice de la part de la plateforme, même dans les cas où la collecte de ces données ne poserait pas de problèmes éthiques. Ces considérations d'ordre juridique rendent ainsi difficile l'utilisation de méthodes de recherche systématique permettant de surmonter les obstacles liés à la fragmentation. De même, des obstacles d'ordre éthique limitent la mesure dans laquelle les chercheurs peuvent utiliser des méthodes qualitatives pour étudier légitimement les communautés nuisibles sur Discord malgré l'absence d'obstacles d'ordre juridique. Les questionnaires auxquels il faut généralement répondre afin d'entrer dans les groupes peuvent nécessiter une tromperie importante ou la promotion de croyances problématiques. C'est particulièrement le cas pour les petits serveurs, le seuil de tolérance concernant les attentes raisonnables en matière de protection de la vie privée n'étant pas clairement défini.

Ces obstacles se cumulent pour limiter la portée des résultats de nos recherches, qui reposent principalement sur des observations qualitatives et non systématiques provenant de serveurs dont les considérations éthiques ne nous

ont pas empêchés de les rejoindre en premier lieu. Nos résultats indiquent néanmoins une présence significative de contenus haineux, antidémocratiques et violents au sein de ces communautés.

Les sections suivantes décrivent l'histoire et les fonctionnalités de Discord, les méthodes de recherche que nous avons explorées et utilisées, les limites que nous avons rencontrées et les résultats de notre analyse.

Vue d'ensemble de la plateforme

Discord a été lancé en 2015 en tant que plateforme gratuite de jeux vidéo et a été conçu pour aider les joueurs à communiquer entre eux pendant qu'ils jouent. Depuis, le nombre d'utilisateurs de Discord a connu une croissance spectaculaire. Il est actuellement estimé à 6,7 millions de serveurs actifs et 140 millions d'utilisateurs actifs mensuels à travers le monde.[29]

Fonctionnalités principales

Discord permet aux utilisateurs de se parler en temps réel au moyen de messages texte ou de chats vocaux ou vidéo entre utilisateurs. Les chat rooms, connus sous le nom de serveurs, peuvent être créés par n'importe quel utilisateur à des fins qui vont au-delà du jeu en ligne, notamment la mise en réseau, l'organisation d'événements et de concours, les discussions thématiques, les raids (campagnes organisées pour spammer ou troller d'autres serveurs ou utilisateurs sur d'autres plateformes), ainsi que la collecte et le partage de contenus qui intéressent les membres des serveurs.

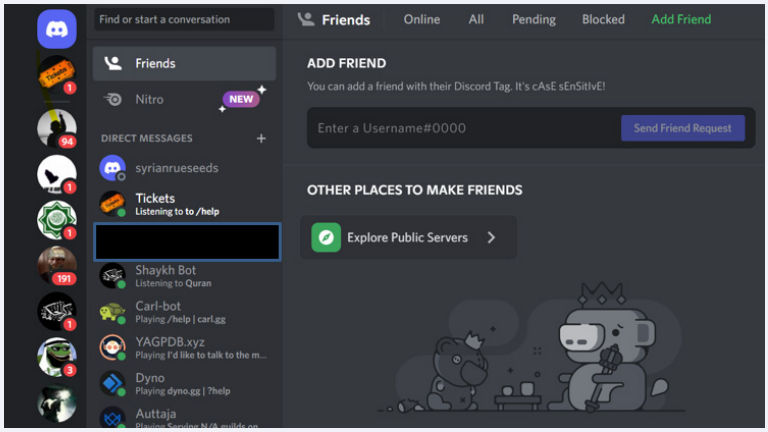


Figure 10: Interface utilisateur de Discord.

Beaucoup de ces serveurs sont privés, mais beaucoup sont également publics (bien qu'il faille toujours un nom d'utilisateur pour les rejoindre). Les plus grands serveurs publics peuvent compter des centaines de milliers de membres.[30] Si de nombreux serveurs publics sont consacrés aux jeux ou aux anime, d'autres sont dédiés aux discussions sociales ou politiques (certains discutent explicitement et s'inspirent de thèmes et d'une esthétique similaires à ceux de communautés que l'on trouve sur d'autres plateformes comme 4chan).[31]

Activités préjudiciables sur Discord

Bien que Discord soit principalement destiné aux joueurs et conçu à des fins non politiques, des chercheurs ont constaté que l'application avait également été utilisée par divers groupes extrémistes. Par exemple, avant le rassemblement meurtrier des suprémacistes blancs à Charlottesville en Virginie en août 2017 (au cours duquel un militant d'extrême droite a assassiné un contre-manifestant en lançant délibérément une voiture sur la foule), les organisateurs avaient utilisé Discord pour planifier et coordonner la manifestation, ainsi que pour partager des documents de propagande idéologique.[32]

À la suite de rapports sur l'utilisation de Discord par l'extrême droite, et sur les événements de Charlottesville en particulier, Discord a commencé à adopter une approche plus stricte vis-à-vis de la présence de ces mouvements sur sa plateforme.[33] En 2021, Discord a affirmé avoir supprimé plus de 2 000 serveurs extrémistes.[34] Cependant, des recherches menées plus tard par l'ISD dans la même année ont révélé que Discord servait toujours de plaque tournante pour la socialisation et la construction de communautés d'extrême droite, même s'il y a peu de preuves que le jeu en lui-même ait eu un rôle dans les stratégies dangereuses de radicalisation et de recrutement de nouveaux individus sur la plateforme.[35] De plus, les recherches ont permis d'identifier, sur les serveurs Discord d'extrême droite, des expressions de soutien à la Division Atomwaffen et à la Division Sonnenkrieg (deux organisations considérées comme terroristes au Royaume-Uni, au Canada et en Australie).[36]

Alors que Discord semble particulièrement populaire parmi les adhérents de l'extrême droite, il est aussi utilisé par les membres d'une communauté plus jeune d'extrémistes islamistes de la génération Z qui allient les idées salafistes[ii] avec les mèmes de l'extrême droite et les sous-cultures de gamer.[37] Le rôle joué par Discord dans diverses sous-cultures en ligne adeptes de l'extrémisme et de la violence a été mis en lumière en 2022 par l'attentat de Buffalo et la fusillade lors du défilé à Highland Park. Dans les deux cas, l'empreinte numérique des attaquants contenait des messages laissés sur Discord ainsi que des contenus prouvant la planification et la préparation leur attaque.[38]

Étude de Discord

Méthodologie de recherche

Discord présente des obstacles à la fois d'ordres juridique et éthique (principalement pour les méthodes quantitatives et qualitatives respectivement lors de l'étude de groupes privés) et liés à la fragmentation (à la fois pour les groupes publics et privés), car les recherches sur la plateforme ne peuvent être effectuées que serveur par serveur et non de façon systématique. Pour contourner ces obstacles, les chercheurs ont adopté deux approches méthodologiques différentes : 1) l'accès systématique aux données limitées aux serveurs d'intérêt spécifique et 2) la recherche ethnographique.

Comme indiqué ci-dessus, des recherches antérieures menées par l'ISD sur Discord avaient montré qu'à la fois les extrémistes islamistes et l'extrême droite étaient présents sur la plateforme. Les chercheurs de l'ISD se sont demandé si le projet pourrait avoir pour objectif l'analyse complète des groupes d'extrême droite, étant donné que les recherches précédentes sur Discord avaient révélé une présence significative de l'extrême droite sur la plateforme. Cependant, il a été décidé qu'une étude plus restreinte et plus ciblée de sous-communautés spécifiques au sein de l'extrême droite pourrait contribuer davantage aux actions menées par les chercheurs pour comprendre la diversité des communautés extrémistes et la dynamique de radicalisation sur Discord. Compte tenu des rapports faisant état d'un intérêt croissant de l'extrême droite américaine pour des concepts tels que l'intégrisme et le traditionalisme catholiques, y compris parmi les adeptes des mouvements d'extrême droite America First et Groyper qui ont mobilisé sur Discord,[39] l'ISD a choisi de se concentrer sur les contenus haineux et violents au sein des serveurs intégristes et traditionalistes catholiques.[iii] Cette étude a été complétée par une analyse des communautés islamistes extrémistes

ii Le salafisme est une forme d'islam sunnite dont les adeptes prônent un retour aux pratiques des trois premières générations de musulmans (les salaf ou « ancêtres ») qui ont vécu juste après le prophète Mahomet. Au sein du salafisme, il existe de multiples courants qui divergent significativement dans leurs interprétations des écritures saintes de l'islam et de leurs implications pour l'action politique. Parmi les salafistes, on distingue souvent les salafistes quiétistes, qui rejettent l'activisme politique, les salafistes politiques, qui s'engagent activement dans la transformation de la société selon leur pensée idéologique, et les salafistes djihadistes, qui utilisent la violence pour mettre en œuvre une interprétation salafiste de la loi islamique.

iii L'intégrisme catholique est une tendance du catholicisme qui rejette la séparation entre le pouvoir séculier et le pouvoir religieux. Les finalités spirituelles étant supposées plus importantes que les finalités temporelles, les intégristes affirment que les enseignements de l'Église devraient déterminer la politique pour servir le bien commun. L'intégrisme catholique n'est pas une tendance récente, mais ces dernières années ces idées ont progressé dans les communautés (en ligne) anglophones d'extrême droite. Dans une certaine mesure, ces idées rejoignent celles des traditionalistes catholiques, qui rejettent l'adhésion partielle de l'Église catholique à la modernité (en particulier sur des questions telles que la liberté de religion, le rôle des hommes et des femmes et les droits de l'homme, ainsi que sur la liturgie) consécutive au concile Vatican II entre 1962 et 1965, certains traditionalistes ne reconnaissant plus la légitimité des papes qui se sont succédé depuis et/ou la légitimité de leurs enseignements. Par exemple, les sédévacantistes considèrent que la papauté est restée vacante depuis le concile Vatican II, tandis que le sédéprivationisme admet que le pape est légitimement élu mais qu'il manque d'autorité en raison d'erreurs doctrinales. Les tendances distinctes du sédévacantisme et de l'intégrisme peuvent se rejoindre dans une certaine mesure en raison de leurs positions anti-laïques, anti-libérales et anti-pluralistes, ainsi que de leur rejet des réformes du concile Vatican II. Les idées intégristes catholiques sont discutées sur un large éventail de plateformes, y compris sur Discord.

sur Discord, ce qui nous a permis de déterminer quelles méthodologies étaient applicables et à quels obstacles les chercheurs pouvaient être confrontés en tentant d'accéder aux données de communautés nuisibles dont la présence sur Discord avait déjà été documentée.

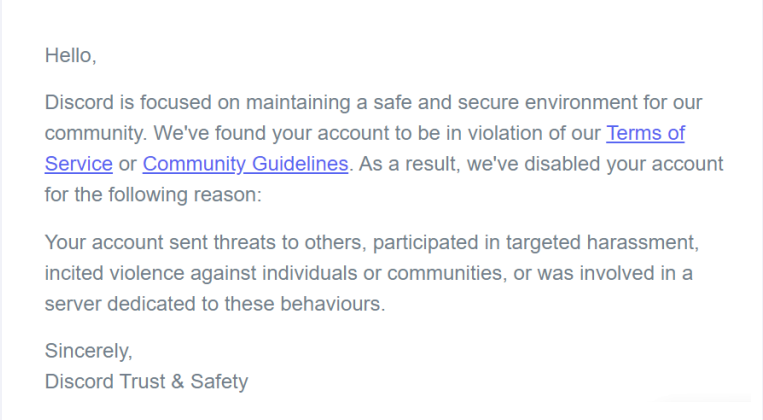
Pour identifier les serveurs Discord liés à l'extrémisme catholique et islamiste, nous avons procédé en deux étapes. Tout d'abord, les chercheurs ont créé des listes de mots-clés associés à l'extrémisme catholique et islamiste en ligne en utilisant les fonctions de recherche de la plateforme Discord, ainsi que Disboard (un outil open source indépendant de Discord mais qui permet aux utilisateurs de trouver des serveurs).[40] Des listes de mots-clés ont été créées sur la base de recherches antérieures de l'ISD sur l'extrémisme islamiste et d'un examen des publications et rapports existants sur l'extrémisme catholique dans les pays anglophones.

En s'appuyant sur cette première étape, les chercheurs ont ensuite entrepris une recherche manuelle « de fil en aiguille » sur chaque plateforme (c'est-à-dire en utilisant les cas initiaux pour découvrir et développer de nouveaux cas). Les chercheurs se sont appuyés sur les serveurs recommandés dans les discussions extrémistes, et en particulier sur les serveurs « partenaires ». Des chats de partenariat sont utilisés au sein des serveurs pour dresser la liste des serveurs partageant les mêmes idées et qui se promeuvent mutuellement auprès de leurs membres parce que considérés comme étant pour eux potentiellement intéressants. Les descriptions des partenariats sont généralement beaucoup plus détaillées que celles figurant sur Disboard et permettent habituellement aux chercheurs de tirer des conclusions indicatives sur leur contexte idéologique probable.

En suivant ces étapes, les chercheurs ont identifié 31 serveurs catholiques et 16 serveurs islamistes extrémistes. Pour classifier l'idéologie des serveurs, les chercheurs de l'ISD ont évalué leur nom, leurs tags sur Disboard et/ou leurs descriptions. Dans de nombreux cas, un serveur n'est pas dédié à une idéologie particulière, mais comporte un mélange de différents points de vue qui expriment des désaccords importants tout en débattant d'autres sujets plus anodins. Il est donc plus approprié de décrire la majorité des serveurs que nous avons étudiés comme des communautés dans lesquelles des voix extrémistes se font entendre plutôt que comme des serveurs extrémistes en tant que tels.

Pour cette étude de cas, deux comptes ont été créés. Cela a permis d'éviter les soupçons des autres utilisateurs de ces serveurs, car il est possible de voir sur combien de serveurs (et lesquels) un utilisateur partage la même adhésion avec d'autres. Par exemple, il serait suspect que les chercheurs qui rejoignent des serveurs extrémistes islamistes soient déjà membres de serveurs extrémistes catholiques.

Il convient de noter que notre compte créé pour étudier les communautés catholiques extrémistes sur Discord a été suspendu deux mois après avoir rejoint les serveurs identifiés. Discord a déclaré que le compte était en « violation de nos conditions d'utilisation ou de nos règles communautaires ». Bien que la raison précise n'ait pas été donnée, il semble, d'après la liste de comportements fournie, que la suspension ait été motivée par le fait que d'autres membres


Hello,

Discord is focused on maintaining a safe and secure environment for our community. We've found your account to be in violation of our Terms of Service or Community Guidelines. As a result, we've disabled your account for the following reason:

Your account sent threats to others, participated in targeted harassment, incited violence against individuals or communities, or was involved in a server dedicated to these behaviours.

Sincerely,
Discord Trust & Safety

Figure 11: Notification de Discord sur la suppression du compte de recherche de l'IDS.

de ces serveurs envoyaient des menaces, participaient à du harcèlement ciblé ou incitaient à la violence. Nombre des serveurs analysés étaient susceptibles d'avoir eu un ou plusieurs de ces comportements, mais aucune information n'a été fournie, ni sur le serveur qui a conduit à cette décision, ni sur l'éventuelle suppression de ce serveur. Plusieurs des 31 serveurs catholiques extrémistes que les chercheurs de l'ISD avaient rejoints n'étaient plus disponibles via la fonction de recherche de Discord ou via Disboard lorsque nous avons mis fin à notre collecte de données en août 2022 (nous ne sommes cependant pas entièrement convaincus que cela signifie nécessairement qu'ils aient été supprimés par la plateforme).

Comme Discord dispose d'une API accessible de façon publique, nous avons étudié la possibilité d'accéder systématiquement aux données en vue d'une analyse plus approfondie des serveurs identifiés comme pertinents au cours de ces étapes. Les sections suivantes décrivent les obstacles liés à la fragmentation ou d'ordres juridique et éthique que nous avons rencontrés.

Obstacles liés à la fragmentation

Sur Reddit, Facebook et d'autres plateformes, il est possible d'accéder aux discussions des groupes publics par le biais de l'API. Cela signifie qu'un chercheur peut trouver rapidement des mentions de mots-clés pertinents dans toute une série de groupes publics. Discord n'offre pas de fonctionnalité aussi étendue. Il est possible de rechercher et de télécharger des messages via l'API de Discord, mais cela ne peut se faire que serveur par serveur. Certains utilisateurs ont automatisé cette opération pour qu'elle fonctionne à grande échelle.[41] Il apparaît cependant que les chercheurs devraient connaître à l'avance les canaux dans lesquels ils souhaiteraient effectuer des recherches. Étant donné le grand nombre de canaux sur Discord et le fait que les canaux qui hébergent des contenus ou des comportements préjudiciables sont parfois supprimés et/ou renommés, la recherche systématique peut s'avérer très difficile. Pour être clair, le souci ici n'est pas que les informations soient cachées, car elles seraient faciles à trouver si le chercheur savait en amont où chercher. Discord présente donc pour les chercheurs des obstacles liés à la fragmentation.

De plus, la manière dont les fonctions de recherche sur Discord ou Disboard fonctionnent n'est pas transparente, en ce qui concerne la manière dont leurs résultats sont déterminés, le degré d'exhaustivité des résultats et quels résultats sont absents. Disboard regroupe aussi les serveurs au moyen de tags qui indiquent quels serveurs sont susceptibles de contenir des idéologies nuisibles (par exemple : l'État islamique, le djihad, les talibans, le califat et le salafisme). Le nom et la description de chaque serveur ont été examinés manuellement afin de déterminer s'ils étaient susceptibles d'être pertinents pour ce projet.

Deux facteurs montrent que les fonctions de recherche ne sont complètes ni sur Discord ni sur Disboard. Tout d'abord, elles produisent des résultats très différents, ceux de Disboard étant généralement beaucoup plus complets. Ensuite, même dans les résultats de Disboard, des divergences inexpliquées apparaissent souvent entre le nombre de serveurs prétendument identifiés et le nombre de serveurs réellement affichés. Il est donc concevable que leur fonctionnalité de recherche limite la précision des données qu'ils fournissent, ce qui pourrait fausser nos résultats.

Obstacles d'ordres éthique et juridique

Discord présente plusieurs obstacles d'ordres éthique et juridique. Une plateforme pourrait présenter les obstacles éthiques spécifiques à Discord sans pour autant présenter les obstacles juridiques que nous avons rencontrés et inversement.

Obstacles d'ordre éthique

Comme sur Telegram, l'admission sur des serveurs sur Discord peut nécessiter de répondre d'une manière trompeuse aux questionnaires, qui sont très couramment utilisés pour se renseigner sur les nouveaux arrivants qui tentent de rejoindre des communautés dédiées. Fournir des réponses trompeuses à ces questionnaires de vérification

est particulièrement problématique dans le cas de petits serveurs dont les utilisateurs peuvent avoir des attentes raisonnables en matière de protection de la vie privée.

En créant des comptes pour la recherche et la conduite ultérieure de recherches ethnographiques, l'ISD s'efforce toujours de minimiser les pratiques trompeuses. Des photos de profil ou des informations sur le sexe ou les centres d'intérêt ne sont fournies que si nécessaire, et cela doit être justifié au cas par cas. En outre, les noms de compte doivent être des pseudonymes, afin de protéger les chercheurs mais aussi d'éviter tout préjudice à des tiers. Les pseudonymes (ou autres informations fournies conformément aux principes énoncés ci-dessus) utilisés dans les comptes ne doivent pas être identifiables à ceux d'une personne réelle.

À défaut de passer par la procédure de vérification, les utilisateurs sont confinés dans une zone d'attente. L'étendue des informations sur le serveur qui sont déjà visibles depuis la zone d'attente varie considérablement. La plupart des serveurs disposent d'un questionnaire de vérification des nouveaux utilisateurs (seuls 8 des 47 serveurs que nous avons évalués n'avaient pas de procédure de vérification). Les questionnaires consistent généralement en une poignée de questions. Après avoir examiné ces questionnaires, l'ISD les a classés en plusieurs catégories, en fonction du degré de tromperie et d'idéologie que nécessitent les réponses.

- **Niveau 1** : Questions ne nécessitant aucune information sur les opinions politiques et/ou religieuses des utilisateurs.
- **Niveau 2** : Questions portant sur l'identité de l'utilisateur, mais sans rien de particulièrement sensible (par exemple, « Quelle est votre religion ? » ou « Sur quel continent vivez-vous ? »).
- **Niveau 3** : Questions portant sur l'identité de l'utilisateur et exigeant en outre des réponses qui développent les opinions religieuses, politiques ou idéologiques de l'utilisateur (par exemple : « Veuillez décrire vos opinions politiques » ou « Pratiquez-vous activement votre religion ? »).
- **Niveau 4** : Questions spécifiques et sensibles sur l'identité des utilisateurs, nécessitant des réponses qui démontrent un accord religieux, politique ou idéologique (par exemple : « Soutenez-vous les attentats suicides ? » ou « Êtes-vous d'accord pour haïr tout péché et toute perversion ? »).

Les chercheurs de l'ISD ont généralement répondu à des questions relevant des niveaux 1 ou 2 (21 serveurs). Dans tous les cas à l'exception d'un, l'ISD a été autorisé à rejoindre le serveur. Pour le seul cas où l'accès n'a pas été accordé, les administrateurs du serveur ont posé d'autres questions concernant les croyances politiques et religieuses qui auraient nécessité des niveaux de tromperie injustifiables pour y répondre.

Un problème éthique similaire est que les questionnaires demandent souvent aux utilisateurs s'ils sont d'accord avec les règles propres au serveur. Ces règles peuvent elles-mêmes être très controversées, y compris celles qui, par exemple, interdisent certaines religions ou certains mouvements politiques ou préconisent la ségrégation des sexes. Les personnes qui déclarent accepter ces règles peuvent être considérées comme les approuvant.

Un autre problème éthique qui se pose sur les petits serveurs est de savoir à partir de quel seuil débutent les attentes raisonnables en matière de respect de la vie privée. Discord n'est pas le seul concerné par ce problème : les groupes WhatsApp sont limités à 256 membres, Signal autorise des groupes de messagerie non sécurisée comptant jusqu'à dix membres et des groupes comptant jusqu'à mille membres, et les profils Facebook peuvent avoir jusqu'à 5 000 amis. Ces groupes en ligne peuvent tous être considérés comme privés (bien que cela dépende des paramètres dans le cas de Facebook). Cela montre que la ligne de démarcation entre les espaces publics et privés est plus ou moins arbitraire, car il n'existe pas de limite quantifiée reconnue au-delà de laquelle un espace privé devient un espace public. La taille des serveurs Discord est très variable, les plus grands serveurs apolitiques pouvant compter des centaines de milliers de membres. Plus fréquemment, les plus petits serveurs comptent des centaines ou des milliers de membres. De nombreux serveurs extrémistes religieux identifiés par l'ISD n'ont que des centaines, voire que des dizaines de membres. Par conséquent; faute de définition claire de la limite entre les canaux de communication

privés et publics y compris sur la base du nombre d'utilisateurs ou de participants, il est évident que beaucoup de ces communautés extrémistes sur Discord opèrent dans une zone grise à l'égard de ce qui peut être raisonnablement considéré comme étant un espace privé en ligne.

Obstacles d'ordre juridique

Le client API de Discord permet aux utilisateurs de se connecter à un serveur et de collecter aussi bien les messages en ligne du canal que les messages archivés. Pour se connecter à un serveur, les chercheurs ont le choix entre deux méthodes pour s'identifier. La première consiste en un compte bot qui nécessite d'être accepté personnellement sur le serveur par un administrateur (par exemple le créateur du serveur ou un autre membre disposant de ce privilège) susceptible de refuser l'accès. De plus, le bot sera clairement identifié comme tel dans la liste des utilisateurs, ce qui peut susciter des soupçons, notamment au sein des communautés débattant de sujets sensibles ou controversés, partageant des contenus illégaux ou menant des activités illégales.

La deuxième méthode possible est de lancer un bot caché derrière un compte utilisateur normal (un « self-bot »). Dans ce cas, les chercheurs s'inscrivent sur le serveur en tant qu'utilisateur normal (par exemple à l'aide d'un lien d'invitation), et le bot se fait ensuite passer pour cet utilisateur. Cette supercherie viole les conditions d'utilisation de Discord.[42] Les conditions d'utilisation renvoient également à la politique de la plateforme à l'égard des développeurs, qui interdit le scraping, c'est-à-dire la collecte en masse de données à partir d'un serveur Discord (« Vous ne pouvez en aucun cas utiliser les API pour récupérer des données Discord »).[43] Pour mener des recherches ethnographiques sur Discord (c'est-à-dire mener des recherches en agissant en tant qu'observateur ou participant dans un groupe), les chercheurs doivent créer un compte d'utilisateur. En s'inscrivant sur Discord, les utilisateurs s'engagent à respecter les conditions d'utilisations de la plateforme. La plateforme Discord présente donc des enjeux juridiques pour la recherche, car la collecte trompeuse de données sur les canaux via l'API peut être considérée comme une atteinte au droit des contrats, ce qui pourrait entraîner des poursuites juridiques de la part de la plateforme.

Analyse des communautés Discord : principaux résultats

La fragmentation et les obstacles d'ordres éthique et juridique décrits dans les sections précédentes ont limité la portée de nos recherches. Les résultats de nos recherches reposent ainsi principalement sur des observations qualitatives et non systématiques provenant de serveurs dont les considérations éthiques ne nous ont pas empêchés de faire partie en premier lieu. Les recherches indiquent néanmoins une présence significative de contenus haineux, antidémocratiques et violents au sein de ces communautés.

Vue d'ensemble des serveurs

Les sections suivantes décrivent les résultats de nos recherches ethnographiques sur les communautés catholiques et islamistes extrémistes sur Discord. Nous commençons par donner une vision d'ensemble de la taille, de la nature et du caractère de ces communautés. Nous détaillons ensuite des exemples de discours haineux et violents que nous avons identifiés.

Fin août 2022, les chercheurs de l'ISD ont constaté un soutien aux opinions extrémistes catholiques sur 31 serveurs Discord avec un total de 9 585 abonnés et un soutien à l'extrémisme islamiste sur 16 serveurs Discord avec un total cumulé de 4 757 abonnés. Il convient de réaffirmer que même si la création d'une communauté est l'un des principaux objectifs de Discord, il existe une grande diversité au sein des serveurs. Il est donc plus juste de dire que notre analyse s'est concentrée sur les activités liées à l'intégrisme catholique et à l'extrémisme islamiste sur des serveurs Discord où d'autres sujets sont également abordés, plutôt que sur des serveurs exclusivement consacrés à l'intégrisme catholique ou à l'extrémisme islamiste.

Malgré cela, les règles des serveurs stipulent souvent que les commentaires ne doivent pas violer les enseignements religieux, offenser les croyants ou attaquer les autorités religieuses, et que les utilisateurs peuvent être exclus s'ils enfreignent ces règles. De plus, la plupart des serveurs recourent abondamment à l'ironie et à la gamification (c'est-à-dire l'utilisation d'éléments de jeux vidéo pour faciliter la radicalisation, promouvoir des opinions extrémistes ou concevoir des contenus extrémistes ou terroristes). Il est souvent difficile de savoir si les utilisateurs soutiennent réellement des États ou des mouvements religieux autoritaires ou s'ils les trouvent simplement esthétiquement intéressants ou « sympas ».[44]

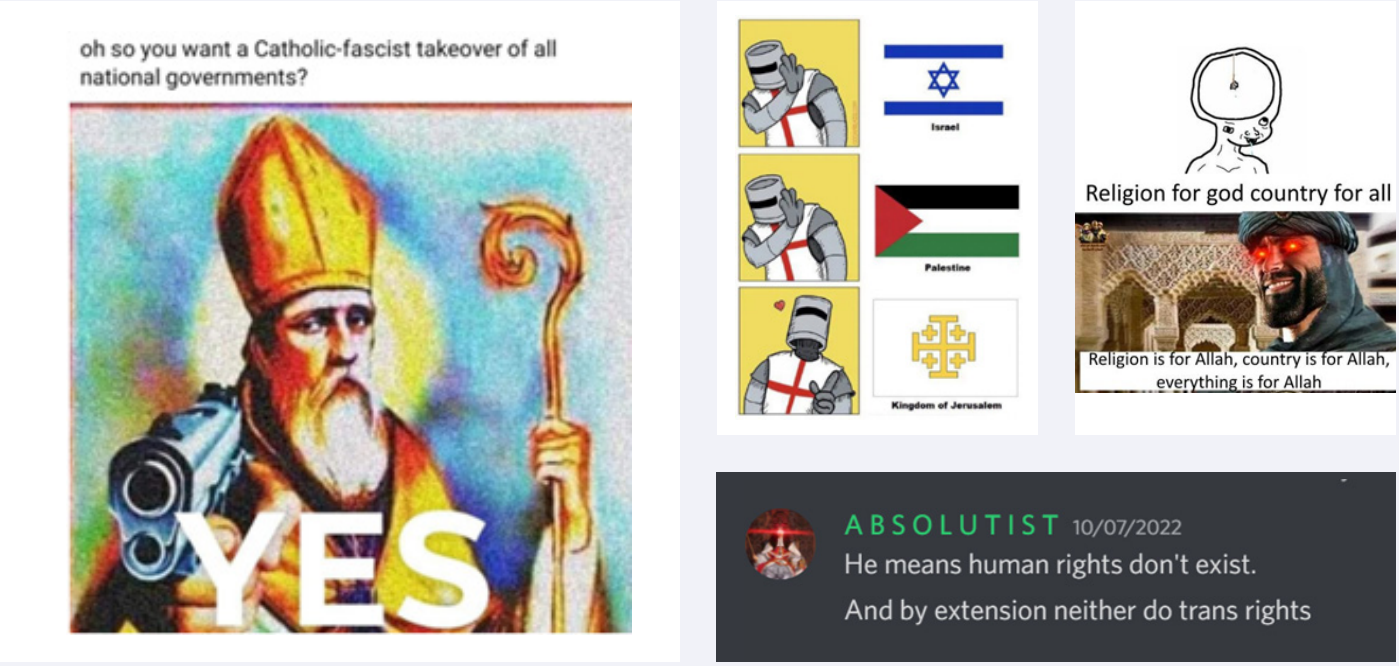


Figure 12: Contenu et mèmes partagés sur les serveurs Discord catholiques et islamistes exprimant une opposition aux droits de l'homme et aux droits des personnes transgenre, ainsi qu'un plaidoyer en faveur d'un État religieux totalitaire.

Les utilisateurs des serveurs extrémistes catholiques et islamistes décrivent souvent leur vision d'une société idéale. Parfois, les administrateurs la définissent également dans les règles propres au serveur. Conformément à la définition de l'extrémisme de l'ISD (voir glossaire), ces visions utopiques revendiquent généralement la supériorité et la domination d'un groupe d'appartenance identitaire (catholique ou musulman) sur tous ceux qui ne font pas partie de ce groupe, faisant ainsi la promotion d'une vision du monde qui semble incompatible avec le pluralisme et les droits de l'homme universels. La forme précise que prendrait l'État catholique idéal n'est pas claire. Les chercheurs ont identifié entre autres des utilisateurs soutenant notamment des intégristes anticapitalistes de gauche, des fascistes, des monarchistes et des nationalistes chrétiens.

Parmi les extrémistes islamistes, les appels au rétablissement d'une version moderne et totalitaire du califat qui unifierait tous les musulmans sont également fréquents. Dans ce califat, tous les aspects de la vie, y compris les questions politiques, scientifiques et spirituelles, seraient soumis aux interprétations islamistes extrémistes de l'islam. Il s'agit notamment d'une interprétation légaliste stricte de la charia, comprenant des châtiments corporels et des limites à la liberté de croyance, à la liberté d'expression et aux droits des minorités sexuelles et religieuses. Les extrémistes islamistes sunnites présents sur les serveurs Discord analysés méprisent particulièrement les musulmans chiites, les soufis, les athées et les musulmans libéraux.

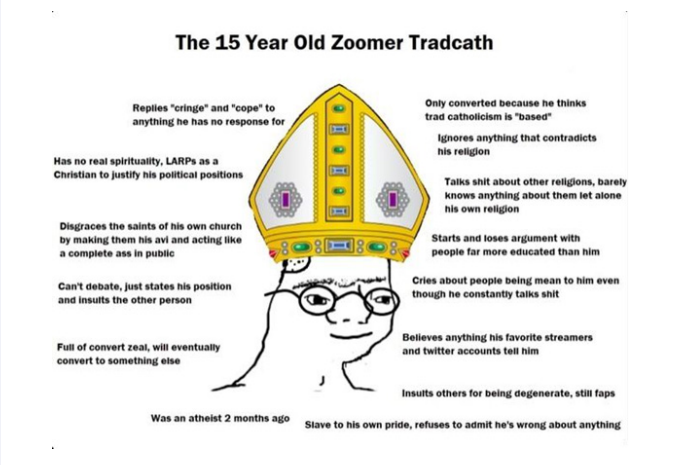


Figure 13: Mèmes ironiques qui se moquent des clichés liés aux sous-cultures catholiques extrémistes en ligne.

Rhétorique haineuse

La section suivante présente différents types de contenus haineux et offensants à l'égard de communautés particulières qui ont été identifiés sur divers serveurs. Alors même que la vision positive de la société peut faire l'objet de vifs débats, certains autres groupes identitaires et ennemis politiques sont régulièrement visés. La distanciation semble être essentielle à la formation d'une identité de groupe et à l'affirmation de ce qui est considéré comme « normal » ou « based ».[iv]

Certains administrateurs de serveurs semblent conscients que les tendances idéologiques de leurs communautés pourraient entrer en conflit avec les politiques de Discord concernant les discours haineux ou la promotion de contenus extrémistes violents. Par exemple, deux serveurs catholiques ont demandé à leurs membres, dans leurs règles, d'essayer de ne pas cibler les groupes protégés ou les communautés BAME (« Black, Asian and Minority

iv '« based » est un terme d'argot qui signifiait à l'origine « addict au crack ». Ce terme a d'abord été repris par le rappeur Lil B pour désigner la façon de « se comporter de manière authentique », puis par l'extrême droite en ligne pour décrire ce qui est conforme à ses valeurs anti-progressistes

Ethnic », probablement un serveur basé au Royaume-Uni où cet acronyme a été le plus couramment utilisé) afin d'éviter d'enfreindre les conditions d'utilisation de Discord.[v]

La haine à l'égard des communautés LGBTQ est un facteur commun sur lequel se rejoignent les utilisateurs catholiques et islamistes extrémistes de Discord. Malgré les divergences idéologiques entre les serveurs sur de nombreux thèmes, il semble exister un quasi-consensus sur le rejet de l'homosexualité et des droits des personnes transgenre. Dans des discussions sur des serveurs catholiques et islamistes extrémistes, les utilisateurs exprimaient généralement ce qu'ils considéraient comme étant la position normative de leur religion.

Figure 14: Commentaires et mèmes anti-LGBTQ se réjouissant de la peine de mort pour les homosexuels en les montrant en train de se faire pousser d'un toit et en se moquant de l'idée que les écritures islamiques seraient compatibles avec les droits des personnes LGBTQ.

Sur Discord, les serveurs extrémistes catholiques et islamistes se rejoignent sur le thème de l'antisémitisme. Tous deux mettent souvent l'accent sur un antisémitisme fondé sur la religion et s'appuyant sur des formes persistantes et historiques d'antisémitisme. Alors que les discours antisémites des extrémistes islamistes sont parfois plus ou moins liés à la haine d'Israël, la plupart des contenus antisémites des extrémistes catholiques et islamistes sur Discord n'ont aucun lien avec Israël et dépeignent plutôt les Juifs comme des satanistes (ou même comme contrôlant Satan), des démons, des êtres cupides ou des sous-hommes. D'autres contenus (voir figure 15) affirment que le judaïsme n'est pas seulement démoniaque, mais qu'il est également lié à la défense des droits des personnes transgenre. Il s'agit d'un sujet de débat très prisé dans les cercles d'extrême droite selon lequel les juifs tenteraient d'affaiblir les sociétés patriarcales en détruisant les normes binaires de genre.

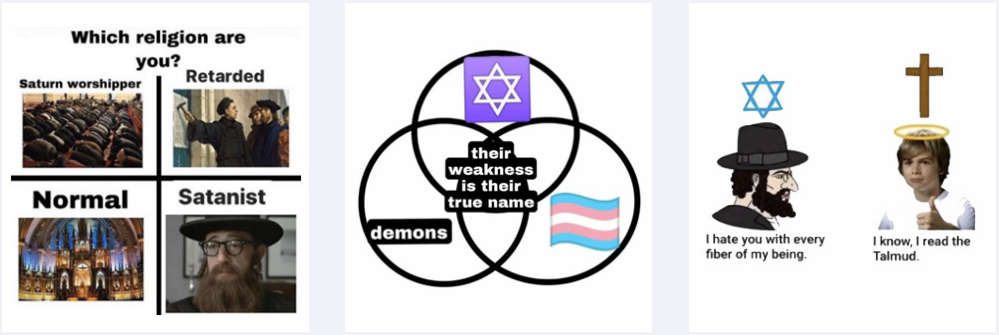


Figure 15: Mèmes attaquant les juifs, les protestants, les musulmans et les personnes transgenre.

v Les Community Guidelines (règles communautaires) de Discord stipulent ce qui suit : « Ne pas organiser, promouvoir ou participer à des discours ou des comportements haineux. Il est inacceptable d'attaquer une personne ou une communauté sur la base de caractéristiques telles que sa race, son ethnie, sa caste, son origine nationale, son sexe, son identité de genre, sa présentation de genre, son orientation sexuelle, son appartenance religieuse, son âge, ses maladies graves, ses handicaps ou d'autres catégories protégées ». « Discord Community Guidelines » [Règles communautaires Discord], Discord, février 2023, https://discord.com/guidelines.

Figure 16: Mème ironisant sur les femmes qui ne se conforment pas au partage traditionnel des rôles entre hommes et femmes, et capture d'écran d'une vidéo fantasmant sur l'assassinat de Malala Yousafzai, défenseuse des droits des femmes.

Les serveurs catholiques et islamistes extrémistes sur Discord, ainsi que les membres de ces serveurs, se rejoignent dans leur opposition au féminisme. Les utilisateurs se moquent souvent des féministes ou se plaignent qu'elles se laissent guider par leur point de vue sur les normes en matière de genre. Prétendre que les normes traditionnelles en matière de genre et de famille rendraient les femmes plus heureuses, alors que les valeurs féministes aboutissent à ce que les femmes deviennent vieilles, sans enfants, solitaires et pleines de regrets est un angle d'attaque courant contre le féminisme.

L'opposition à l'avortement est une autre critique du féminisme et des droits de la femme que l'on retrouve plus fréquemment sur les serveurs catholiques extrémistes (alors même qu'il existe une certaine diversité d'opinions au sein de l'islam comme entre les islamistes, l'opposition absolue à l'avortement est relativement rare). Les utilisateurs des serveurs catholiques approuvaient généralement le rejet de l'arrêt Roe contre Wade de juin 2022, un serveur intégriste de gauche dénonçant même le droit à l'avortement comme « individualiste et inhérent au libéralisme », arguant que c'était la raison pour laquelle Nikita Khrouchtchev avait légalisé l'avortement dans le cadre de ses réformes de « déstalinisation » dans les années 1950. Sur certains serveurs islamistes extrémistes qui soutiennent les talibans, les utilisateurs ont également exprimé leur opposition au droit des femmes à l'éducation. Une vidéo imaginait un retour dans le passé pour s'assurer que les assassins de Malala Yousafzai avaient été suffisamment bien formés pour la tuer.[vi]

Rhétorique violente

S'agissant de la classification des contenus violents, il convient de tenir compte du fait que les utilisateurs puissent adopter des positions qui demeurent plutôt constantes plutôt que de traiter le soutien à la violence comme une variable binaire. Il peut s'agir d'un besoin implicite de violence, de faire l'éloge ou de soutenir des délinquants ou des groupes violents connus, d'appeler à rejoindre des mouvements violents, d'appeler à la violence de manière non ciblée, voire de proposer du matériel pédagogique et des informations susceptibles d'exposer des individus ou des groupes à la violence.

Alors qu'il n'y avait que peu d'appels à la violence, les chercheurs ont identifié une série d'appels à la violence non ciblés, d'éloges de la violence et de messages sous-tendant un besoin de violence, en particulier sur les serveurs Discord des extrémistes islamistes. Par exemple, des utilisateurs ont formé le vœu que Dieu permette aux moudjahidines de tuer des homosexuels et leurs sympathisants ou encore de provoquer une véritable insurrection contre

vi Malala Yousafzai est une militante pakistanaise des droits de l'homme et lauréate du prix Nobel de la paix sur laquelle les talibans avaient tiré en 2012 en raison de son militantisme en faveur du droit de chaque enfant, et notamment des filles, à recevoir une éducation.

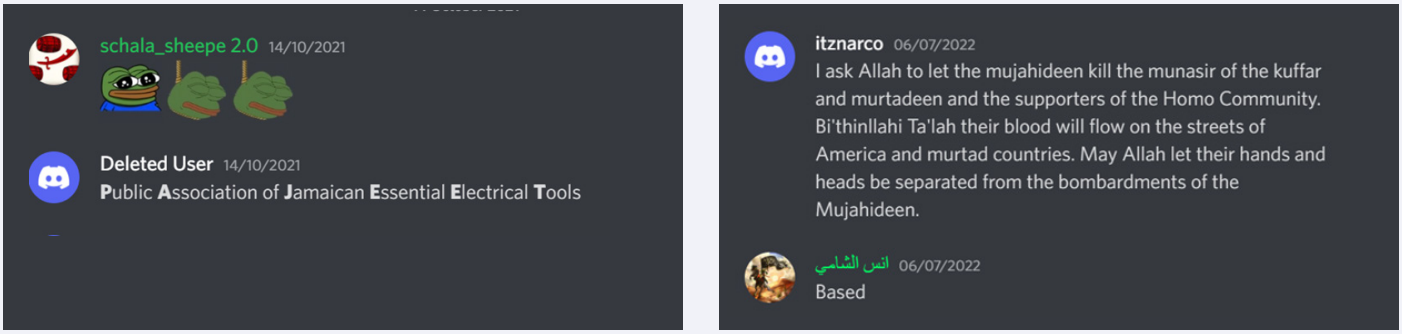


Figure 17: Commentaires appelant à l'exécution d'Indiens (symbolisés par le nom Pajeet) et invoquant Dieu pour tuer les homosexuels.

l'État pakistanais. Certains mèmes dépeignaient l'assassinat d'Occidentaux ou la pendaison d'Hindous (représentés par des personnages de Pepe la grenouille nommés Pajeet, un terme péjoratif utilisé en ligne pour désigner les Indiens).

Sur les serveurs extrémistes islamistes, les utilisateurs exprimaient également leur soutien à des organisations extrémistes et terroristes, notamment à l'État islamique, à Al-Qaïda, aux talibans et au Hamas. Ils partageaient notamment des contenus officiels de l'État islamique et des talibans (y compris des vidéos d'exécutions) et créaient leurs propres mèmes et graphismes de jeux vidéo faisant l'éloge de groupes extrémistes ou terroristes. Il est intéressant de noter que les contenus et commentaires favorables à l'État islamique semblent particulièrement susciter la polémique, voire des réactions plus critiques que les déclarations favorables à d'autres mouvements islamistes extrémistes. Ainsi, les talibans semblent bénéficier d'un plus grand soutien, avec une grande diversité de mèmes se réjouissant du rétablissement réussi de l'Émirat islamique d'Afghanistan en septembre 2021.

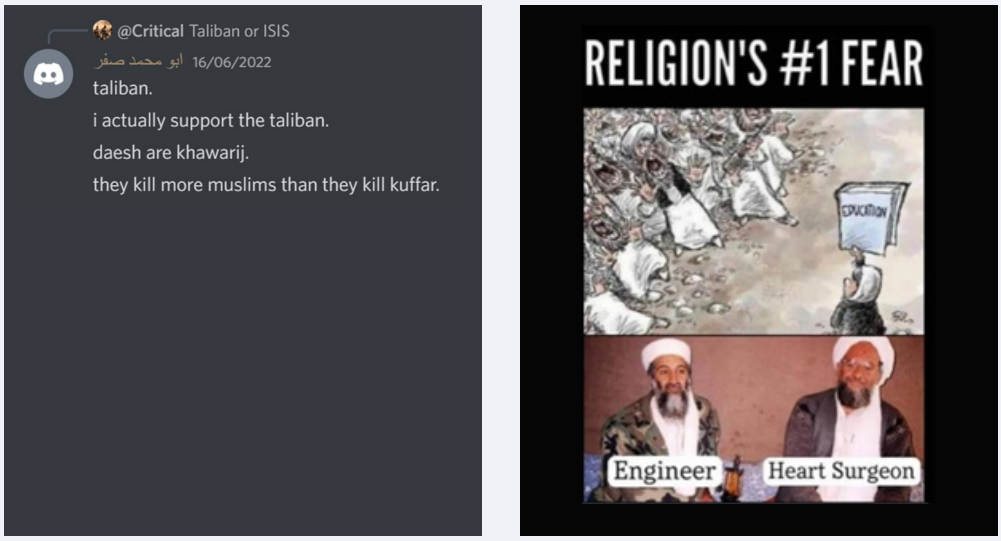


Figure 18: Messages exprimant un soutien aux talibans et ridiculisant l'idée que la religion pourrait être affaiblie par l'éducation en soulignant que les dirigeants décédés d'Al-Qaïda, Oussama ben Laden et Ayman al-Zawahiri, avaient reçu une formation d'ingénieur pour le premier, et de chirurgien cardiaque pour le second.

Cela n'implique pas l'existence d'une idéologie cohérente au sein des serveurs analysés. Premièrement, les différents groupes extrémistes sont souvent opposés les uns aux autres. Par exemple, les talibans, Al-Qaïda et le Hamas sont tous opposés à l'État islamique. Dans le cas de l'Afghanistan, par exemple, les talibans et ISIS-K (la branche afghane de l'État islamique) sont engagés dans des combats militaires les uns contre les autres. Deuxièmement, comme indiqué précédemment, il existe souvent une diversité de points de vue idéologiques au sein des serveurs, et les désaccords entre les utilisateurs sont fréquents.

Figure 19: Mèmes et graphismes de jeux vidéo exprimant un soutien aux talibans.

La rhétorique violente était moins fréquente sur les serveurs catholiques intégristes analysés. Parfois cependant des utilisateurs et des administrateurs laissaient entendre que la violence était nécessaire pour lutter contre la « dégénérescence et la société moderne ». Dans un de ces cas, un utilisateur avait partagé des propos du tireur de l'église de Charleston, Dylann Roof, qui demandaient aux lecteurs de commencer à se battre pour la « race blanche » plutôt que pour de supposés intérêts juifs (voir la section précédente sur la rhétorique haineuse). Enfin, certains mèmes concernaient la figure mythique de saint Jacques le tueur de Maures et célébraient les meurtres de musulmans.

Figure 20: Contenu basé sur la figure mythique de saint Jacques le tueur de Maures, se réjouissant du meurtre de musulmans, et une citation de Dylann Roof, le tireur de l'église de Charleston.

Résultats et recommandations

Notre analyse des serveurs Discord catholiques et islamistes extrémistes montre qu'il existe une présence faible mais significative de communautés nuisibles qui partagent parfois des contenus extrêmes, haineux, antidémocratiques et violents. En raison des obstacles dus à la fragmentation, des préoccupations éthiques et des risques juridiques, les résultats de nos recherches restent qualitatifs et non-systématiques, et ne montrent probablement qu'une fraction de l'ampleur réelle des activités similaires sur la plateforme.

Les obstacles d'ordre éthique sont compréhensibles dans le contexte des préoccupations relatives à la vie privée et aux droits de l'homme, mais les décideurs politiques, les plateformes et les défenseurs des droits de l'homme devraient collaborer pour élaborer des définitions plus simples et plus faciles à mettre en œuvre des espaces publics

et privés qui mettent en balance ces préoccupations avec la recherche d'intérêt public sur l'extrémisme et d'autres activités en ligne préjudiciables.

Nous soutenons que les risques juridiques liés aux violations potentielles du droit des contrats que présentent les conditions d'utilisations de Discord empêchent la recherche légitime d'intérêt public sur les activités en ligne préjudiciables. Il serait souhaitable que les plateformes, y compris Discord, modifient leurs conditions d'utilisation pour permettre une recherche systématique dans l'intérêt du public, plutôt que de se protéger efficacement du contrôle public. Il serait préférable que le gouvernement adopte une législation visant à protéger les chercheurs des risques juridiques lorsqu'ils mènent des recherches d'intérêt public sur des communautés nuisibles opérant dans des espaces publics en ligne.

Enfin, Discord devrait coopérer avec Disboard pour 1) améliorer les fonctionnalités de recherche et 2) identifier et modérer de manière proactive les serveurs qui contiennent des activités illégales ou contreviennent aux conditions d'utilisation de Discord en utilisant la fonction de taggage de Disboard.

Étude de cas n° 3 : **Odysee**

Principaux résultats

- Odysee est une plateforme principalement audiovisuelle basée sur la technologie de la blockchain. Nous avons donc étudié Odysee en tant qu'exemple potentiel d'obstacles technologiques.
- Nous avons découvert que la nature basée sur la blockchain d'Odysee présentait moins d'obstacles insurmontables que nous aurions pu imaginer. En effet, la visibilité publique des transactions utilisant la cryptomonnaie LBC a fourni des points de données supplémentaires. Cependant, cela a nécessité une expertise technique et un travail considérable pour étudier et combiner ensemble différents outils. La nature audiovisuelle de la plateforme présentait également des défis, les chercheurs devant en inspecter le contenu manuellement.
- Comme Odysee offre actuellement moins de modération que les plateformes audiovisuelles traditionnelles, en plus de la monétisation potentielle du contenu et des options d'importation de vidéos depuis YouTube, Odysee pourrait devenir un site populaire pour le contenu audiovisuel lié à l'extrémisme ou aux théories du complot.

Pour l'étude de cas portant sur les communautés extrémistes francophones, l'ISD a mené des recherches sur les communautés néo-fascistes et royalistes (ainsi que sur un groupe de fondamentalistes catholiques liés à ces deux courants) sur Odysee, une plateforme qui présente principalement des obstacles d'ordre technologique. Comme les plateformes décentralisées et/ou basées sur la blockchain comme Odysee demeurent un territoire relativement inexploré de la recherche en ligne, nous avons essayé de voir si les méthodes de recherche systématiques étaient applicables, quelles données pouvaient être disponibles et quels obstacles supplémentaires se poseraient durant le processus.

Au début de ce projet de recherche, nous ne savions pas exactement quels types de données seraient disponibles via l'API LBRY d'Odysee (voir ci-dessous) ou si la nature décentralisée de la plateforme pouvait poser des problèmes de synchronisation des points de données. Il s'avère que LBRY donne accès aux détails des portefeuilles, aux détails des blocs, des transactions, et aux détails des canaux et des vidéos. Cependant, des obstacles technologiques existent encore. Par exemple, il n'est pas possible de voir immédiatement si une vidéo a été importée depuis une autre plateforme, comme YouTube, ou postée à l'origine sur Odysee. Il n'existe à cette fin que des méthodes imparfaites.

Au cours de nos recherches, nous avons identifié des obstacles juridiques supplémentaires à la recherche sur Odysee. Les conditions d'utilisation de la plateforme limitent la collecte de données personnelles mais ne fournissent pas une définition claire de ce que cela signifie dans ce contexte et qui puisse être mise en œuvre. Étant donné que les données en question sont publiquement accessibles et visibles sans se connecter à un compte Odysee, les considérations d'ordre éthique concernant la protection de la vie privée sont limitées. Il n'est cependant pas certain que la collecte de ce qu'Odysee définit comme des données personnelles violerait le droit des contrats.

Ces obstacles se combinent pour limiter les points de données qui peuvent être recueillis pour cette étude de cas et la manière dont ils peuvent ensuite être présentés. Pour les besoins de cette recherche, nous avons décidé de recueillir des données qui ont été publiées publiquement, telles que des vidéos et des commentaires, et de les regrouper en catégories d'utilisateurs. Nos résultats indiquent une présence d'idéologies extrémistes antidémocratiques au sein des communautés francophones sur la plateforme. Cette présence inclut des documents négationnistes et vénérant le national-socialisme, qui tous deux peuvent constituer des infractions pénales en France.

Les sections suivantes décrivent l'histoire et les fonctionnalités d'Odysee, les méthodes de recherche que nous avons explorées et utilisées, les limites que nous avons rencontrées et les résultats de notre analyse.

Vue d'ensemble de la plateforme

Odysee est une plateforme vidéo qui se positionne comme une alternative à YouTube. En décembre 2020, la plateforme revendiquait 8,7 millions d'utilisateurs.[45] Bien que la plateforme ne soit pas exclusivement utilisée par des extrémistes et des théoriciens du complot, elle est devenue populaire parmi ceux qui ont été bannis des grandes plateformes vidéo pour avoir violé leurs conditions d'utilisation, Odysee voulant se présenter comme ayant une approche plus indulgente de la modération du contenu que les plateformes plus populaires.[46] Par exemple, lorsqu'on leur a demandé pourquoi ils permettaient à la chaîne russe RT (maintenant sanctionnée au sein de l'UE) de continuer à utiliser leur service, Odysee a déclaré qu'ils « voul[aient] permettre [à] des voix concurrentes [de s'exprimer] dans le journalisme ».[47] Cependant, un récent rapport de l'antenne allemande de l'ISD a constaté que Odysee bloquait en réalité trop de contenu et restreignait des comptes entiers à cause de quelques vidéos qui violaient les règles communautaires, tandis que certains contenus illégaux restaient visibles pour les adresses IP allemandes.[48] Odysee a pris ses distances avec l'étiquette « alt-tech », laquelle est associée à une proximité idéologique avec l'extrême droite, préférant le nom de « new-tech » (nouvelles technologies).[49]

Odysee est le successeur d'une plateforme vidéo appelée LBRY.tv et fonctionne sur le réseau LBRY, un protocole de partage de fichiers et de paiement basé sur la blockchain détenu par LBRY Inc. Selon son propre site Internet, LBRY veut faire pour la publication de contenu en ligne « ce que le Bitcoin a fait pour l'argent », c'est-à-dire créer une alternative aux plateformes établies décentralisée, promettant ainsi aux utilisateurs un contrôle plus grand sur leurs créations.[50] Comme le réseau LBRY est un protocole blockchain, cela signifie théoriquement que le contenu ne peut pas être modéré par une autorité centrale, bien qu'Odysee modère certains contenus en pratique. LBRY a également sa propre monnaie appelée LBRY Coin (LBC) que les utilisateurs peuvent gagner en téléchargeant des vidéos et en recevant des interactions avec leur contenu. Comme LBRY est une blockchain publique, ces transactions financières sont visibles, ce qui est important pour les chercheurs. Nous détaillons ci-dessous la façon dont cela peut être utilisé.

Le PDG de LBRY Inc., Jeremy Kauffman, était précédemment candidat au Sénat du New Hampshire pour le Parti libertarien aux États-Unis en 2022.[51] L'affiliation de LBRY au libertarisme contribue probablement à la perception parmi les utilisateurs que la plateforme ne poursuit qu'une modération limitée.[52] En octobre 2021, Odysee a annoncé qu'elle développerait son activité indépendamment de LBRY mais qu'elle continuerait à utiliser son protocole et sa cryptomonnaie. Odysee a un PDG distinct et fonctionne via une filiale de LBRY appelée Odysee Holdings Inc.[53] L'objectif du nouveau PDG et ancien employé de TikTok Julian Chandra est apparemment de faire passer Odysee de l'espace libertaire à un public plus traditionnel afin de le rendre rentable.[54]

Fonctionnalités principales

Comment Odysee héberge du contenu

Odysee sert principalement à télécharger des vidéos mais peut également être utilisé pour distribuer d'autres formats de fichiers comme le texte ou l'audio. Pour télécharger ou interagir avec du contenu, les utilisateurs doivent créer un compte et ainsi accepter les conditions d'utilisation d'Odysee.[55] Cependant, il est possible qu'il y ait des vidéos sans attribution sur la plateforme (c'est-à-dire qu'il peut y avoir des vidéos pour lesquelles la personne qui les a téléchargées est anonyme ou dont le compte n'est plus accessible). Les utilisateurs peuvent également importer leurs vidéos depuis YouTube en synchronisant leurs chaînes lors de leur inscription à Odysee.

Bien que la page d'accueil d'Odysee offre une grande variété de contenu, à la fois politique et non politique, elle présente parfois des figures politiques controversées, ce qui renforce l'idée selon laquelle les idéologies extrémistes marginales et la désinformation sont acceptées sur la plateforme. La barre latérale d'Odysee propose différentes catégories de contenu, dont beaucoup sont liées aux loisirs et aux modes de vie. Cependant, la section « Actus & Politique » inclut des chaînes telles que RT, Sputnik et The Alex Jones Channel, ce qui renforce l'hypothèse selon laquelle Odysee ne modèrerait pas les contenus manifestement et intentionnellement faux.

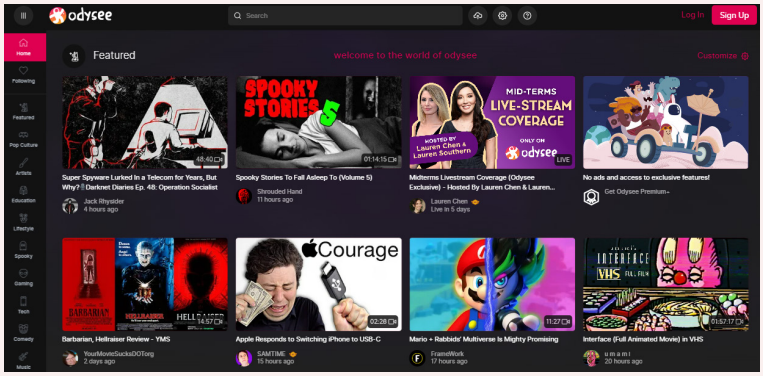


Figure 21: Page d'accueil d'Odysee (03/11/2022).

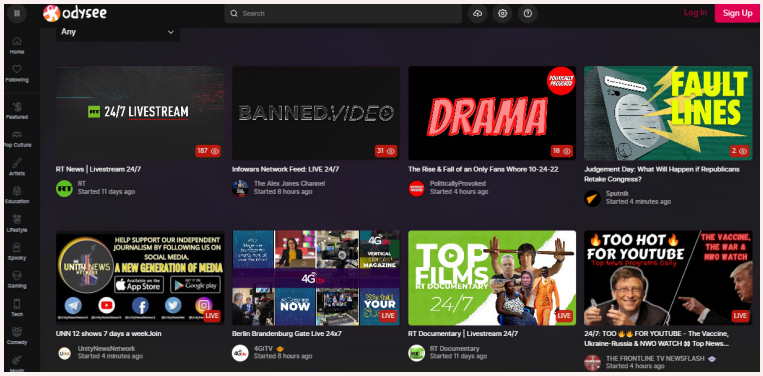


Figure 22: Section « Actus & Politique » d'Odysee (08/11/2022).

Monétisation

Odysee permet aux créateurs de monétiser leur contenu avec la cryptomonnaie LBC mentionnée ci-dessus. La cryptomonnaie LBC peut être échangée contre des monnaies officielles comme le dollar américain sur des plateformes de trading de cryptomonnaies. Fin octobre 2022, 1 LBC ne valait que 0,02 dollar américain. Les transactions sur la blockchain LBRY sont publiques, et il est donc possible de déterminer combien un utilisateur a gagné en LBC sur Odysee. Chaque compte est accompagné d'un portefeuille LBC, et chaque vidéo d'un identifiant de transaction.

L'utilisation de la blockchain par Odysee (afin de transférer plus facilement la monnaie d'un portefeuille à un créateur de contenus sur la même plateforme) abaisse le seuil de monétisation par rapport aux plateformes non basées sur la cryptomonnaie comme YouTube. Ces plateformes nécessitent des partenariats plus formels avec les créateurs pour permettre la monétisation, ce qui permet également aux plateformes de retirer la capacité des créateurs à monétiser le contenu s'il est jugé non adapté aux annonceurs. En conséquence, l'utilisation de la blockchain par Odysee rend potentiellement la plateforme attrayante pour ceux qui sont interdits de monétiser leur contenu sur d'autres plateformes.

Bien qu'Odysee ne diffusait pas à l'origine de publicités, elle a annoncé en octobre 2021 qu'elle commencerait à diffuser des publicités sur les vidéos, avec la promesse de prendre une part plus petite de recettes que d'autres entreprises.[56] La plateforme propose également un plan premium avec visionnage sans publicité et diverses autres fonctionnalités.

Activités préjudiciables sur Odysee

De nombreuses plateformes qui s'autoproclament libres de toute censure ont tendance à attirer des utilisateurs qui ont été bannis par d'autres plateformes pour avoir publié du contenu extrémiste ou de la désinformation. Les

plateformes qui partagent cette vision, comme Odysee, peuvent choisir de ne pas supprimer ces utilisateurs en raison d'une conviction idéologique, parce qu'elles peuvent gagner de nouveaux utilisateurs lorsque les fans des individus bannis les rejoignent sur la nouvelle plateforme d'hébergement, ou parce qu'elles manquent tout simplement de ressources ou d'expertise pour adopter une approche plus complète de la modération. La plateforme Odysee a été mal perçue par les médias français comme étant une plateforme de choix pour les théoriciens du complot qui avaient été bannis de YouTube pour avoir publié de fausses affirmations sur la pandémie de COVID-19. Le « documentaire » de désinformation en langue française Hold-Up est apparu sur Odysee après avoir été retiré de YouTube. Plusieurs figures de proue de l'extrême droite, comme le politicien Florian Philippot, ainsi que des organes de désinformation comme France-Soir, ont établi des chaînes sur Odysee. La monétisation étant disponible pour tout utilisateur, Odysee présente un risque potentiel en tant que plateforme de financement d'activités antidémocratiques, même si le taux de change actuel pour le LBC est relativement bas.

Étude d'Odysee

Méthodologie de recherche

Bien qu'il ne semble pas qu'il existe une API spécifique à Odysee, les données nécessaires pour mener ces recherches sur Odysee pourraient être accessibles via des API construites pour LBRY. Nous avons étudié deux des outils que LBRY fournit pour interagir avec la blockchain et le réseau LBRY : Chainquery et LBRY SDK.

- **Chainquery** : Il s'agit d'un outil pour interroger les données des transactions sur la blockchain. Bien qu'il soit facile d'utilisation pour un chercheur, Chainquery nécessite l'accès à une copie locale de la blockchain LBRY, ce qui nécessite une configuration et une maintenance difficiles, y compris un matériel informatique plus puissant. Il existe aussi des préoccupations supplémentaires liées à la sécurité et d'ordre éthique dans le fait de rejoindre le réseau LBRY, car cela nécessiterait de répondre à d'autres utilisateurs interrogeant la blockchain, participant ainsi activement au réseau tout en l'étudiant.

- **LBRY SDK** : Cet outil fournit des ressources pour les développeurs pour créer leurs propres applications pour interagir avec la blockchain. En plus de les interroger, le chercheur peut également interagir avec les données (par exemple, retrouver toutes les parties d'une vidéo qui a été divisée et les télécharger). À l'aide de l'outil LBRY SDK, les utilisateurs peuvent se connecter au réseau et accéder à des informations sur le contenu et les transactions ainsi qu'aux métadonnées associées. Bien que la création de demandes d'accès aux données pour l'API LBRY SDK puisse être plus chronophage, la configuration est plus facile et les exigences de maintenance sont moins élevées.

Pour ce projet, nous avons choisi cette dernière approche pour intégrer Odysee à Method52. Aucun des outils LBRY ne donne accès aux commentaires postés sur Odysee. Cela est géré par un système séparé, Commentron, qui est géré directement par l'équipe Odysee. Le système fournit également une API, qui fonctionne de manière similaire à LBRY SDK. Pour avoir accès aux commentaires vidéo pour la recherche, il était nécessaire d'intégrer également cette API à Method52.

Les chercheurs peuvent également analyser Odysee de manière similaire à d'autres plateformes vidéo. Cela comprend l'examen manuel du contenu vidéo, l'étude de l'historique des propriétaires des canaux et la collecte de statistiques fournies à tous les utilisateurs par la plateforme, telles que le nombre d'abonnés et de téléchargements. Cependant, l'examen manuel du contenu vidéo peut devenir laborieux en présence de grands échantillons de contenus et de comptes. Cet examen ne permet généralement pas non plus une analyse systématique plus détaillée, comme l'étude des pics d'activité autour de certaines périodes.

L'étude manuelle des transactions financières triées selon les acteurs concernés permet aux analystes d'identifier les portefeuilles de cryptomonnaies et leurs soldes. Cependant, cela est à nouveau très chronophage lorsqu'il s'agit d'étudier un grand nombre de comptes. De plus, il existe quelques limites à l'analyse des soldes créditeurs de multiples portefeuilles. Les utilisateurs peuvent posséder plus d'un portefeuille, et il peut donc être difficile de saisir

les véritables revenus financiers d'un seul utilisateur sur la plateforme. De plus, si les chaînes surveillées s'envoient mutuellement des crédits, ces LBC pourraient être comptés deux fois si l'on se contentait de ne comparer que les soldes d'ouverture et de clôture d'un portefeuille.

Pour automatiser le processus de collecte des revenus en LBC, CASM a construit un composant pour Method52 qui collecte les détails des vidéos, notamment les identifiants de portefeuilles et les montants des soutiens (c'est-à-dire combien les utilisateurs ont gagné avec leurs vidéos). En plus de permettre une collecte de données à plus grande échelle grâce à l'automatisation, un autre avantage de cette approche est que les identifiants de portefeuilles peuvent être reliés à des comptes avec une plus grande certitude. L'outil LBRY Block Explorer[vii] ne permet pas d'établir avec certitude à qui appartient chaque identifiant de portefeuille, et les chercheurs utilisant une approche manuelle doivent donc déduire les relations entre les utilisateurs et les portefeuilles en analysant les identifiants de transaction individuels des vidéos. Cela est non seulement chronophage mais ne permet pas non plus de prouver de manière concluante à quel canal appartiennent les identifiants de portefeuilles.

Obstacles d'ordre technologique

La blockchain demeure une technologie émergente et il y a peu de travaux de recherche systématique, basés sur les données sur les plateformes de médias sociaux reposant sur la blockchain. En conséquence, il peut y avoir des résultats inattendus lors de l'utilisation de nouvelles méthodes de collecte de données, et la nature décentralisée de la technologie pourrait conduire à des distorsions dans les données collectées (comme l'ISD l'a découvert lors des travaux de recherche sur une autre plateforme décentralisée, PeerTube). L'utilisation des technologies de la blockchain par les extrémistes préoccupe de plus en plus les chercheurs dans d'autres contextes, par exemple après que les partisans de l'État islamique avaient commencé à utiliser les NFT pour créer de la propagande terroriste impossible à supprimer.[57] Cependant, les commentateurs se sont principalement concentrés sur l'utilisation de la cryptomonnaie plutôt que sur l'utilisation des plateformes reposant sur la blockchain pour la propagande.

Bien qu'Odysee offre également la possibilité de télécharger des fichiers texte (par exemple, des fichiers PDF), il s'agit principalement d'une plateforme vidéo. Le contenu audiovisuel présente un défi particulier en ce qu'il est plus difficile et laborieux d'analyser systématiquement une grande quantité de ce type de contenu. À moins que des sous-titres ne soient disponibles, l'analyse basée sur le texte est généralement limitée aux titres des vidéos, aux descriptions et aux commentaires. Cependant, les sous-titres (en particulier ceux qui sont générés automatiquement) peuvent toujours causer des problèmes en raison d'une bande-son peu claire ou de l'utilisation de plusieurs langues.

Lors de la collecte de données, nous avons rencontré quelques difficultés liées à la configuration d'Odysee en tant que plateforme. La collecte initiale rencontrait une limite une fois que 1 000 vidéos étaient téléchargées depuis un canal. Cela semble être soit une fonctionnalité, soit un bug non intentionnel dans la conception d'Odysee, où seulement 1 000 vidéos sont affichées sur les canaux. Les vidéos plus anciennes ne sont pas supprimées mais ne sont pas visibles sur les canaux. La collecte de données a donc dû être ajustée pour accéder à ces vidéos qui n'étaient pas affichées.

L'écosystème logiciel autour d'Odysee est également décousu et se chevauche lorsqu'il est comparé à de nombreuses autres plateformes en ligne qui offrent un ensemble d'outils plus cohérent pour pouvoir accéder aux données. Bien qu'il existe une variété d'outils officiels disponibles pour interagir avec Odysee, y compris LBRY SDK et Chainquery, les étudier prend du temps et requiert une expertise technique élevée. Ces outils ne sont pas aussi bien documentés et leur mise en œuvre peut donc prendre beaucoup de temps. Ces deux outils offrent beaucoup de fonctionnalités identiques et permettent d'accéder aux données, mais ils diffèrent également d'autres façons, ce qui rend difficile de déterminer lequel est le plus approprié pour différentes fins. Par exemple, pour avoir accès à la fois aux données vidéo et aux commentaires, il a été nécessaire d'intégrer deux API différentes puisque ces systèmes sont gérés séparément par la plateforme.

vii L'outil LBRY Block Explorer est un outil en ligne d'accès public qui permet aux utilisateurs de rechercher à la fois des informations en temps réel et des informations dans l'historique d'une blockchain, notamment des données relatives aux blocs, aux transactions ou aux adresses.

Dans l'ensemble, les obstacles techniques à la recherche posés par Odysee n'étaient pas aussi prohibitifs que nous l'avions initialement prévu. Les recherches précédentes de l'ISD sur la plateforme n'avaient pas tenté d'employer une approche plus technologique. Cependant, bien que nous ayons pu collecter des données à partir de la plateforme en utilisant des moyens techniques, les obstacles à la conduite de ce type de recherche étaient relativement élevés, nécessitant une expertise technique significative et du temps pour que les chercheurs puissent se familiariser avec la gamme d'options disponibles et les essayer.

Obstacles d'ordres éthique et juridique

Comme la plupart des contenus sur Odysee sont accessibles au public même sans se connecter à un compte, les risques liés à la confidentialité sont limités. Il est raisonnable de supposer que les utilisateurs sont conscients que leur contenu peut être vu par quiconque le trouve. L'outil LBRY Block Explorer qui liste les portefeuilles des utilisateurs est également visible publiquement et montre les soldes des portefeuilles sans avoir à s'inscrire ou à se connecter à des comptes Odysee ou LBRY.

Les principaux problèmes d'ordres éthique et juridique sont liés aux conditions d'utilisation d'Odysee, qui interdisent « la récolte ou autre collecte d'informations sur les utilisateurs, y compris les adresses électroniques, sans leur consentement ».[58] La formulation des conditions d'utilisation n'est pas claire quant aux types de données disponibles qui devraient être considérées comme personnelles et qui ne devraient donc pas être collectées. Les adresses électroniques ne sont pas publiques sur Odysee et il n'est pas possible d'y accéder à l'aide des outils officiels disponibles. Cela soulève des questions sur le fait de savoir s'il est légal et éthique de collecter les différents types de données disponibles, comme les téléchargements et les vues sur l'activité des canaux publics, à condition que les utilisateurs correspondants soient anonymes.

Pour les besoins de ce projet, l'ISD et CASM ont décidé de collecter des données via l'API officielle de LBRY tout en tenant compte des conditions d'utilisation définies par la plateforme Odysee elle-même. Une fois déterminés quels types de données pourraient être collectées grâce à l'API disponible, nous avons évalué lesquelles devraient être considérées comme des données personnelles. Pour ce projet, nous avons décidé de recueillir des données qui ont été publiées publiquement, telles que des vidéos et des commentaires, et de les regrouper en catégories d'utilisateurs. Cette approche a permis d'assurer que les chercheurs ne pouvaient pas identifier des individus précis dans les données, permettant d'atténuer les risques potentiels d'ordres éthique et juridique posés par les conditions d'utilisation d'Odysee concernant la collecte de données personnelles. Cependant, cette approche a empêché l'analyse de certains points de données qui auraient permis une compréhension plus détaillée du comportement des utilisateurs sur la plateforme.

Analyse des communautés Odysee : principaux résultats

Il existe un écosystème vaste mais idéologiquement fragmenté de communautés d'extrême droite et de désinformation francophones sur Odysee. Comme cet écosystème est trop vaste et idéologiquement diffus pour être analysé dans son intégralité, nous nous sommes plutôt concentrés sur trois sous-groupes spécifiques de l'extrême droite française qui ont des connexions idéologiques entre eux, bien que leurs idées ne se rejoignent pas entièrement. Ces factions idéologiques sont les royalistes d'extrême droite, les néo-fascistes et les fondamentalistes catholiques. Les royalistes d'extrême droite ont été choisis en raison de leur importance historique dans la conduite de l'ultranationalisme et de leur opposition à l'ordre politique français actuel. Les néo-fascistes ont été sélectionnés car ils publient fréquemment du contenu qui est illégal, tel que la négation des crimes contre l'humanité commis pendant la Seconde Guerre mondiale. Les fondamentalistes catholiques ont été inclus car il a été observé qu'ils présentaient souvent un pont idéologique entre les deux anciennes communautés en embrassant à la fois l'ethnonationalisme et l'opposition au sécularisme tout en propageant des théories du complot et de la désinformation, comme des contenus contre la vaccination. Tous ces groupes étant enclins à publier des théories du complot sur des élites obscures et s'engageant souvent dans un discours qui dénigre les minorités ethniques ou religieuses, la réputation d'Odysee concernant sa une modération laxiste peut aider à les attirer sur la plateforme.

Les royalistes d'extrême droite s'opposent à l'ordre politique postrévolutionnaire en France, en particulier à l'une des caractéristiques le définissant, la séparation de l'Église et de l'État. La branche la plus radicale des royalistes français soutient un retour à la « loi de droit divin » et à l'absolutisme, où le monarque ne répond que devant Dieu. De telles notions sont intrinsèquement antidémocratiques, le dirigeant ne pouvant être tenu responsable devant aucun pouvoir terrestre, comme le Sénat ou le l'Assemblée nationale française, et les décisions ou les autorités démocratiques pouvant ainsi être écartées. L'expression « extrême droite » dans le contexte français a été utilisée pour la première fois pour désigner les royalistes intransigeants qui, pendant la Restauration post-napoléonienne (1815-1830), étaient assis à l'extrémité droite des bancs.[59]

Les néo-fascistes ne se réfèrent pas nécessairement au fondamentalisme catholique, certains d'entre eux rejetant le christianisme en faveur de croyances néopaïennes. Cependant, il y a néanmoins un chevauchement significatif entre les deux, surtout lorsque les néo-fascistes définissent le peuple de France comme catholique et de pure descendance française et propagent des théories du complot accusant les francs-maçons et les juifs d'activités néfastes ou évoquent des subversions sataniques de la société.

Les chaînes Odysee que nous avons identifiées comme fondamentalistes catholiques se concentrent principalement sur le contenu religieux (souvent sous forme de théories du complot) mais combinent souvent aussi le désir royaliste d'abolir le sécularisme et le soutien néo-fasciste à l'ethnonationalisme. Ils promeuvent parfois même du contenu niant l'holocauste ou d'autres crimes commis pendant la Seconde Guerre mondiale. En fin de compte, toutes ces communautés rejettent les idées des Lumières de l'universalisme et des droits individuels qui ont inspiré la Révolution française et qui définissent toujours la Cinquième République.

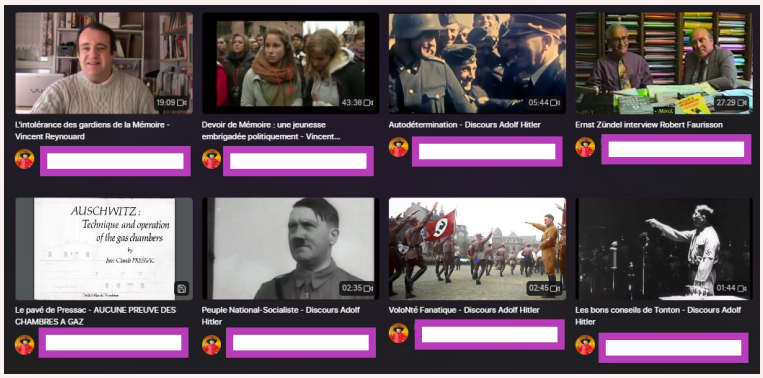


Figure 24: Exemple de contenus d'un canal Odysee néo-fasciste.

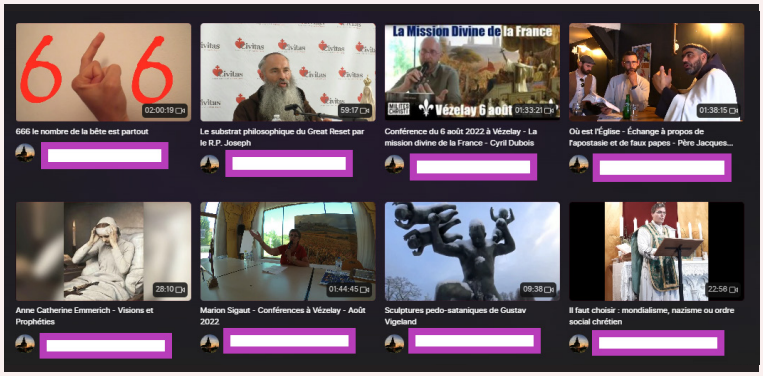


Figure 25: Exemple de contenus d'un canal Odysee fondamentaliste catholique.

Utilisation et engagement sur la plateforme

L'analyse systématique du contenu trouvé au sein de ces communautés pose un défi significatif, même avec l'échantillon relativement limité utilisé pour cette étude. Alors que le texte peut être facilement analysé à l'aide d'un outil NLP capable de classer le texte, le contenu audiovisuel doit d'abord être transcrit. La qualité des outils de transcription peut varier d'une langue à l'autre. Plusieurs personnes parlant en même temps ou plusieurs langues utilisées dans une même vidéo posent généralement des défis considérables pour les programmes de transcription. De plus, les images allégoriques (y compris les signes de ralliement) qui pourraient fournir un contexte supplémentaire important concernant les appartenances idéologiques ou les narrations employées sont susceptibles de passer à la trappe en utilisant cette approche. Pour cette raison, la section suivante examine uniquement les données qui ont pu être collectées en utilisant l'API de LBRY, qui consistent principalement en des statistiques sur les canaux et les vidéos ainsi que les revenus en LBC.

L'analyse des données collectées, qui couvre la période du 1er janvier 2020 au 15 septembre 2022, révèle que le premier pic notable d'activité a eu lieu pendant l'été 2020, ce qui correspond au moment où la plateforme Odysee avait été lancée en remplacement de LBRY.tv. Les données indiquent que l'activité des comptes observés était minime lorsqu'ils étaient sur LBRY.tv. Les premiers pics d'activité après le lancement d'Odysee semblent avoir été principalement provoqués par des téléchargements dans la catégorie néo-fasciste. Les données pour toutes les catégories d'utilisateurs prises ensemble montrent que des augmentations de l'activité quotidienne de téléchargement ont eu lieu à plusieurs reprises depuis la première montée des téléchargements à la fin de l'été 2020, bien que les téléchargements quotidiens se situent généralement entre dix et cinquante vidéos.

Un aspect curieux des données est qu'une grande partie de l'activité de téléchargement tout au long de l'année 2021 provenait des chaînes royalistes, qui sont ensuite devenues le groupe le moins actif en 2022. Néanmoins, avec 8 690 vidéos, ils ont téléchargé le plus de contenu parmi toutes les catégories d'utilisateurs au cours de la période observée d'un peu plus de deux ans et demi. La deuxième catégorie d'utilisateurs la plus active dans l'ensemble était issue des chaînes néo-fascistes, qui ont posté 6 035 vidéos au cours de la période observée. Parmi les trois catégories, ce sont eux qui postaient le plus régulièrement depuis le lancement officiel d'Odysee, avec des périodes d'activité soutenue observables à la fin de l'été 2020, à l'automne 2021 et à l'été 2022.

Les chaînes fondamentalistes catholiques n'ont posté que 4 084 vidéos, bien qu'elles aient clairement augmenté leur taux de téléchargement quotidien au cours de la période observée. Bien qu'il n'y ait eu que quelques téléchargements de cette catégorie d'utilisateurs en 2020 et en 2021, ils sont devenus assez actifs tout au long de l'année 2022. Un pic d'activité particulièrement notable a eu lieu autour de février et mars 2022. Dans l'ensemble, on pourrait déduire de ces données que l'utilisation d'Odysee varie au fil du temps et par catégorie d'utilisateur. Alors que les royalistes semblent avoir perdu leur intérêt pour la plateforme, les fondamentalistes catholiques l'utilisent de plus en plus.

Les commentaires ont été collectés via une API séparée et ne sont montrés qu'à partir de mi-2020. Les différences entre les catégories d'utilisateurs sont également visibles ici bien que le nombre moyen de commentaires et de réponses soit plutôt modeste. Les vidéos des chaînes néo-fascistes recevaient en moyenne 3,3 commentaires, celles des royalistes – 2,4 et celles des fondamentalistes catholiques – 1,5. Cela montre que le taux de téléchargement n'est pas nécessairement lié au nombre de commentaires qu'une certaine catégorie d'utilisateurs recevra.

En examinant le volume au fil du temps, on peut entrevoir une certaine corrélation avec les téléchargements de vidéos, bien que la concordance ne soit pas totale. Alors que les chaînes royalistes étaient très actives dans le téléchargement autour du début de l'année 2021, ces niveaux élevés d'activité ne se reflètent pas dans le taux de publication de commentaires. Néanmoins, leur taux de téléchargement en baisse a été accompagné d'une réduction relative des commentaires. Les vidéos néo-fascistes ont reçu un flux assez régulier de commentaires depuis l'automne 2021. Avant cela, le volume des commentaires était comparativement faible. Il existe occasionnellement

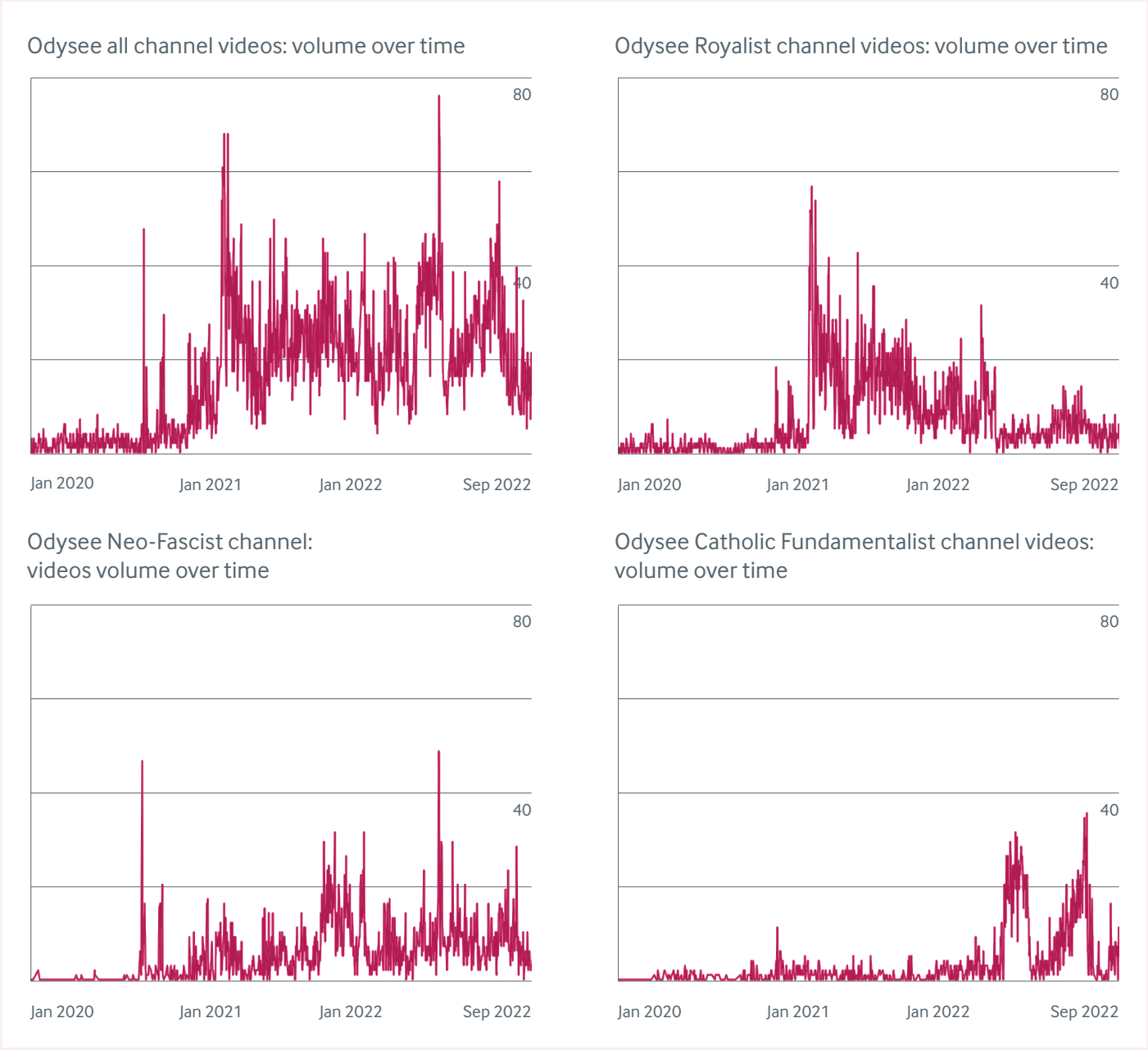


Figure 26: Graphiques montrant les téléchargements de vidéos entre le 01/01/2020 et le 15/09/2022 pour toutes les catégories et par catégorie d'utilisateurs (royalistes, néo-fascistes, fondamentalistes catholiques).

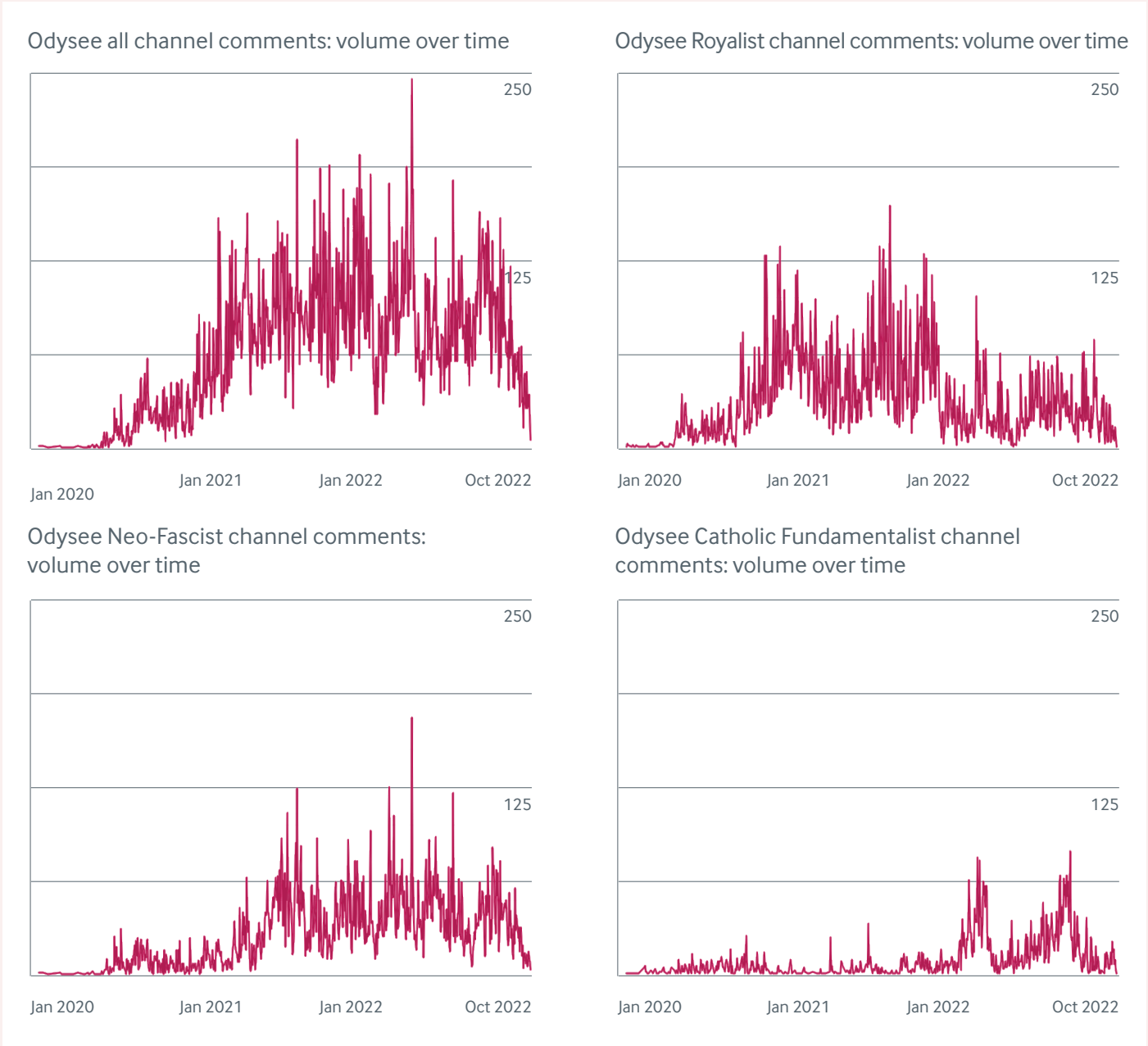


Figure 27: Graphiques montrant la publication de commentaires et de réponses entre le 13/08/2020 et le 15/09/2022 pour toutes les catégories et par catégorie d'utilisateurs (royalistes, néo-fascistes, fondamentalistes catholiques).

des cas exceptionnels lorsqu'un volume particulièrement important de commentaires est posté en une seule journée. La relation la plus proche entre les téléchargements et les commentaires peut être observée parmi les fondamentalistes catholiques qui montrent une activité accrue à la fin de l'hiver et à l'été 2022.

Dans l'ensemble, ces communautés d'extrême droite françaises semblent utiliser Odysee comme une alternative à YouTube. Théoriquement, la plateforme leur permet de gagner de l'argent avec leur contenu plus facilement que sur les plateformes n'utilisant pas de cryptomonnaie. Cependant, compte tenu de la valeur relativement faible du LBC, la réputation d'Odysee de permettre du contenu qui serait supprimé d'autres plateformes pour avoir violé leurs conditions d'utilisation semble actuellement être un facteur plus significatif.

De plus, Odysee offre des options que de nombreuses autres plateformes axées sur la vidéo n'ont pas. Les vidéos peuvent être repostées et sont alors montrées sur la page du canal de l'utilisateur. Cette fonction permet aux chercheurs d'observer les proximités idéologiques et les idées partagées parmi les communautés et d'identifier les narrations qui servent de ponts entre elles. En particulier, cela concerne les théories du complot antisémites et les prétendus complots visant à saper le catholicisme et le peuple français, ainsi que des théories du complot plus globales liées à la « grande réinitialisation » (« Great Reset ») ou au « nouvel ordre mondial » (« New World Order »). Odysee permet également aux utilisateurs de télécharger des fichiers autres que vidéo. Les néo-fascistes utilisent particulièrement cette fonction pour télécharger des documents qui prouveraient que l'holocauste n'aurait pas existé et promouvant des théories du complot antisémites.

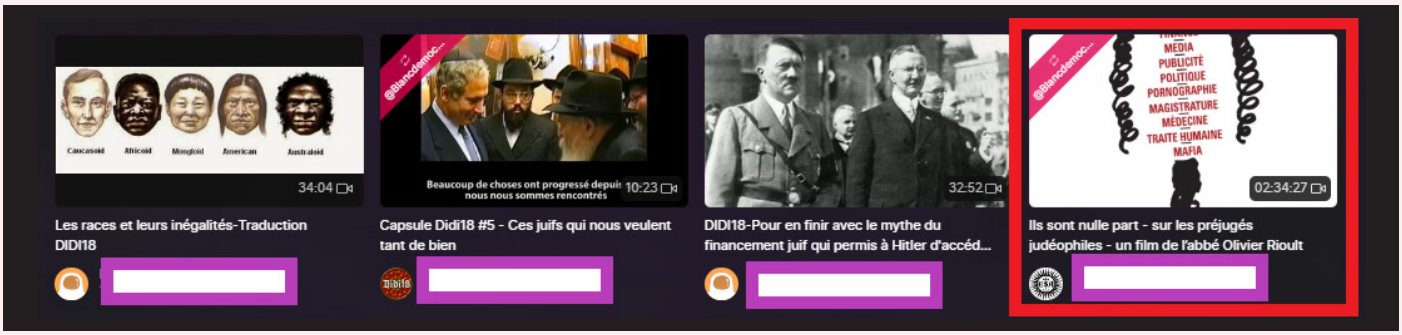


Figure 28: Exemple d'une chaîne néo-fasciste repostant une vidéo antisémite (marquée en rouge) d'un canal fondamentaliste catholique.

Une autre caractéristique spéciale d'Odysee est qu'il permet aux utilisateurs d'importer directement du contenu d'autres plateformes vidéo, comme YouTube. Cette fonction a eu un impact sur les données que nous avons collectées car certaines vidéos avaient des dates de téléchargement datant d'avant l'existence d'Odysee ou de son prédécesseur LBRY.tv. Il n'était pas tout de suite possible de dire clairement à partir de nos données si une vidéo avait été importée depuis une autre plateforme. Afin d'estimer combien de vidéos avaient été importées de YouTube, toutes les descriptions des vidéos ont été recherchées à l'aide de la chaîne « www.youtube.com/watch?v= » et leur volume au fil du temps a été compilé pour analyse. Les vidéos ayant été importées depuis YouTube devraient comporter un lien vers l'URL source de la vidéo sous des pointillés au bas de la description de la vidéo. Bien que cette méthode puisse fournir une approximation du nombre de vidéos importées au fil du temps, elle n'est pas parfaite. Tout d'abord, il peut y avoir des cas dans lesquels la description de la vidéo comporte la chaîne « www.youtube.com/watch?v= », mais qui n'est pas liée à l'importation d'un fichier et qui pourrait simplement faire de la publicité pour une autre vidéo. Ensuite, la date de publication fait référence au téléchargement de la vidéo originale sur YouTube, et non à la date à laquelle la vidéo a été importée sur Odysee. Cela signifie que les graphiques finaux du volume au fil du temps se retrouvent avec un mélange de dates de téléchargement.

L'existence de la fonction d'importation soulève la question de savoir si les acteurs observés tentent de rediriger leur public depuis YouTube vers Odysee, qu'ils pourraient percevoir comme un hôte plus sûr pour leur matériel controversé au cas où des mesures seraient prises contre leurs chaînes par la plus grande plateforme. Sur la base

d'une recherche manuelle et d'une observation anecdotique, il semble y avoir deux tendances qui sont déterminées par le type d'acteur. Premièrement, les acteurs qui servent effectivement de médias alternatifs qui produisent leur propre contenu, comme des podcasts ou des commentaires d'actualités, poursuivent généralement une stratégie multiplateforme, dont Odysee est l'une des multiples alternatives d'hébergement aux plateformes mieux établies. Ces acteurs relient souvent leurs profils à la fois sur les plateformes mainstream et sur les plateformes alt-tech comme Gettr, Telegram et Rumble, et utilisent souvent la fonction d'importation, synchronisant ainsi leurs vidéos entre les plateformes. Il convient de noter que ces acteurs plus organisés ont généralement plus d'abonnés et de vues sur YouTube que sur Odysee. Il semble que ces médias utilisent principalement Odysee comme une sauvegarde parmi d'autres pour garder leur contenu en ligne au cas où leur compte sur une plateforme plus grande serait fermé.

La deuxième tendance concerne les acteurs qui sont passés de YouTube à Odysee ou qui ont toujours été actifs sur Odysee (pour autant qu'on puisse remonter leur trace). Ces comptes publient fréquemment du contenu qui pourrait non seulement enfreindre les conditions d'utilisation de nombreuses plateformes, mais également potentiellement la loi française, notamment les contenus négationnistes et glorifiant le national-socialisme sont concernés. Contrairement à la tendance précédemment mentionnée, ces acteurs ont plus d'abonnés sur Odysee qu'ils en avaient sur YouTube. Alors que sur YouTube ils avaient quelques dizaines et parfois moins de dix abonnés, leurs followers se comptent souvent en milliers sur Odysee. Ces publics ne semblent pas énormes, mais il convient de noter qu'Odysee est une plateforme beaucoup plus petite que YouTube, la première cumulant 23,4 millions de visites mensuelles pour 33 milliards pour la seconde en septembre 2022 selon SimilarWeb.[60] Les chaînes qui présentent des vidéos sur la page d'accueil d'Odysee, qui est censée montrer le contenu le plus populaire du site, peuvent ne compter que dix mille abonnés environ. Ceux qui suivent cette tendance n'importent généralement pas de contenu de leurs chaînes YouTube, la plupart d'entre elles étant inactives depuis des mois lorsque cette recherche a été menée. Au lieu de cela, ces acteurs ont commencé à télécharger directement sur Odysee, ce qui semble avoir offert un nouveau public.

Contrairement au premier groupe d'acteurs, ceux qui sont derrière ces comptes uniquement sur Odysee utilisent généralement des pseudonymes. Ces comptes anonymes téléchargent souvent des contenus d'autres personnes, par exemple des interviews de négationnistes bien connus ou des images historiques idéalisant le Troisième Reich. Une exception est un activiste néonazi connu qui a déjà été condamné en France pour négationnisme mais qui gère toujours ouvertement son propre canal sur Odysee. Si l'on examine les données par le nombre de liens YouTube dans la description des vidéos, les royalistes semblaient en importer le plus (3 595), les fondamentalistes catholiques arrivant en deuxième position (1 807) et les néo-fascistes en important le moins (680). Une explication à cette division pourrait être que de nombreuses chaînes royalistes appartiennent à des groupes organisés et à des médias qui poursuivent une stratégie multiplateforme. En revanche, les néo-fascistes pourraient hésiter à télécharger leur contenu sur YouTube où il est plus susceptible d'être modéré. De plus, comme beaucoup de ces comptes sont anonymes et en grande partie non attribuables, ils sont potentiellement moins intéressés à se promouvoir au moyen d'une stratégie multiplateforme.

Dans tous les cas, Odysee semble principalement servir de moyen pour éviter les interdictions sur les plateformes plus strictement modérées pour ces communautés particulières. Pour les organisations et les médias, Odysee semble servir de moyen pour protéger leur contenu s'ils venaient à être exclus d'autres plateformes. Pour ceux qui publient du contenu ouvertement extrême, Odysee est devenu le principal moyen de diffusion de ce type de contenu. Bien qu'Odysee ait une barre beaucoup plus basse pour la monétisation que YouTube et que beaucoup du contenu examiné ne serait probablement pas monétisé sur les principales plateformes, les éventuels avantages financiers ne semblent pas être le facteur déterminant pour les communautés observées dans leur prise de décision d'utiliser la plateforme. Le revenu en LBC réalisé par ces chaînes depuis le début de notre période de collecte de données en janvier 2020 est négligeable. Au total, les chaînes observées ont gagné moins de 500 dollars américains pour près de 20 000 vidéos en environ deux ans et demi, suggérant qu'Odysee seule ne propose pas (encore) un modèle économique viable pour ces utilisateurs.

Catégorie d'utilisateurs	Nombre de vidéos depuis le 01/01/20	Revenus en LBC depuis le 01/01/20	Conversion en USD (au 22/09/22)
Royalistes	8 690	4 266,733 714	94,66 $
Néo-fascistes	6 035	7 979,900 723	177,03 $
Fondamentalistes catholiques	4 084	7 736,055 632	171,62 $

Résultats et recommandations

Odysee a tenté de se positionner comme une alternative aux plateformes de vidéos en ligne plus traditionnelles comme YouTube tant en termes d'utilisation de la technologie de la blockchain et de paiements en cryptomonnaie qu'en termes de standards de modération laxistes. Nos résultats démontrent qu'Odysee a attiré certaines communautés d'extrême droite françaises, bien que leur présence soit encore relativement faible par rapport à d'autres plateformes, et qu'elles ne semblent pas générer de revenus significatifs en hébergeant leur contenu sur la plateforme. Alors que les conditions d'utilisation d'Odysee interdisent effectivement l'incitation à la haine et à la violence basées (entre autres) sur l'ethnicité, la religion et la nationalité, la présence de contenus ouvertement racistes, antisémites et fascistes indique un manque de mise en œuvre de ces conditions d'utilisation.[61] Certains de ces contenus étant vraisemblablement illégaux dans plusieurs pays, Odysee pourrait être soumis à une pression croissante pour les retirer.

Dans l'ensemble, la technologie de la blockchain sous-jacente à Odysee ne s'est pas révélée être un obstacle aussi sévère à l'accès aux données que nous le craignions initialement. Cela est dû au fait que LBRY fournit une variété d'outils existants pour les développeurs. Cependant, naviguer parmi les outils disponibles pour étudier cette plateforme basée sur la blockchain a toujours nécessité une expertise technique (qui peut ne pas être disponible pour de nombreuses autres organisations) et un temps considérable. Des complications sont survenues en raison de la fragmentation de la technologie sous-jacente d'Odysee, ce qui a rendu nécessaire d'étudier et d'intégrer plusieurs outils pour accéder aux données nécessaires à cette recherche. De plus, tous ces outils n'étaient pas bien documentés ou maintenus aux mêmes normes, augmentant encore l'expertise technologique et les efforts nécessaires. Les plateformes plus petites comme Odysee ont généralement moins de personnel et de ressources financières que les grandes entreprises technologiques pour maintenir ces services. Cela peut entraîner des défis techniques et des incohérences lors de la collecte de données à des fins de recherche. La nouvelle technologie de la blockchain peut aggraver cela car le plus petit nombre d'experts et d'outils disponibles peut signifier que les chercheurs sont forcés d'utiliser des approches moins bien développées et documentées. Dans la mesure du possible, la plateforme devrait chercher à rationaliser cette gamme d'outils et fournir une documentation plus complète, cohérente et accessible pour les accompagner.

Les conditions d'utilisation d'Odysee étaient également particulièrement floues concernant la définition des données personnelles, créant de potentiels obstacles juridiques à la recherche d'intérêt public sur la plateforme. Combiné à la disponibilité d'une grande variété de catégories et de types de données, cela signifie que nous avons adopté une approche plus conservatrice de notre collecte et analyse de données que ce qui aurait pu être techniquement possible. La plateforme devrait clarifier ses attentes concernant l'utilisation des données collectées par les tiers. Cela donnerait plus de certitude aux chercheurs et permettrait aux utilisateurs de mieux comprendre comment leurs données peuvent être utilisées.

Conclusions et recommandations

Dans l'ensemble, les recherches que nous avons menées pour ce rapport démontrent que, bien qu'il soit possible de mener des recherches numériques sur des plateformes telles que Telegram, Discord et Odysee, il peut être difficile de le faire de manière à la fois systématique, éthique et légale. Nous avons néanmoins pu mener des recherches utiles sur chaque plateforme, en particulier avec des méthodes plus manuelles ou ethnographiques. Elles ont été complétées par une collecte et une analyse de données plus systématiques et à plus grande échelle.

Cependant, il y avait également des limites significatives sur chaque plateforme qui empêchaient l'utilisation de méthodes et d'approches de recherche plus complètes. Des considérations éthiques concernant le droit à la vie privée ou des attentes en matière de confidentialité nous ont empêchés de rechercher des communautés Telegram plus petites et plus nuisibles. Des préoccupations juridiques concernant la violation des conditions d'utilisation (et donc du droit des contrats) nous ont empêchés de collecter des données de manière systématique à partir de serveurs Discord. Bien que l'étude d'Odysee ait soulevé moins de problèmes éthiques en raison de sa nature publique, la complexité technique et le manque de clarté des conditions d'utilisation en matière de collecte de données ont également rendu difficile la réalisation d'une analyse plus complète.

Ces obstacles d'ordres technologique, éthique et juridique, et liés à la fragmentation rencontrés sur Telegram, Discord et Odysee sont également profondément liés les uns aux autres et se recoupent. Par exemple, des considérations juridiques nous ont empêchées de surmonter les barrières de fragmentation sur Discord à l'aide de méthodes de recherche systématique, et des fonctionnalités technologiques sur Telegram ont créé d'importants obstacles d'ordre éthique. Les complications liées à l'intégration de plusieurs outils afin de pouvoir accéder aux données d'Odysee ont été aggravées par les conditions d'utilisation de la plateforme, qui sont floues quant à la question de savoir si les différents outils fournissent des données personnelles ou non, créant ainsi une incertitude d'ordres éthique et juridique. Les obstacles éthiques et juridiques limitent donc souvent la capacité des chercheurs à étudier de manière systématique les communautés nuisibles sur ces plateformes, même lorsque de telles approches peuvent être techniquement possibles.

Implications pour les chercheurs

Comme nos recherches l'ont démontré, les plateformes peuvent entraver la recherche d'intérêt public de plusieurs façons, que ce soit de manière délibérée ou involontaire. Comme mentionné ci-dessus, des termes juridiques flous peuvent créer des charges ou des risques supplémentaires pour les chercheurs. Les choix technologiques peuvent empêcher l'accès aux données ou aux contenus hébergés mais également rendre la collecte de données inutilement fastidieuse d'un point de vue technique, par exemple lorsque les architectures front-end (côté interface) ou back-end (côté serveur) des plateformes sont fragmentées ou mal entretenues ou que les outils disponibles pour accéder aux données sont mal documentés. La façon dont les plateformes sont conçues peut également créer une incertitude d'ordre éthique, par exemple lorsque les plateformes ou espaces en ligne sont désignés comme privés mais sont en pratique facilement et largement accessibles à la fois aux utilisateurs et aux chercheurs.

Nos recherches lors de ce projet ont nécessité une expertise considérable de la part de CASM pour explorer les différentes possibilités techniques sur Discord et sur Odysee en particulier. Tous les chercheurs ne disposent pas d'une telle expertise, en particulier dans la société civile. Nous avons également bénéficié de l'accès à une aide juridique pro bono qui nous a permis d'évaluer plus soigneusement les conditions d'utilisation des plateformes et les risques juridiques éventuels liés à l'accès aux données. Cela augmente indubitablement les coûts et les obstacles à la conduite de travaux de recherche sur ces plateformes. Étant donné la grande variété de ces obstacles qui se présentent et se combinent sur différentes plateformes, chaque plateforme est susceptible de présenter un ensemble unique et souvent complexe de difficultés pour les chercheurs. Pour illustrer l'ampleur du défi pour les chercheurs, dans le rapport de la phase initiale publié dans le cadre de ce projet, nous avions identifié 81 plateformes ou services en ligne uniques liés aux communautés extrémistes anglaises, françaises et allemandes que nous avons examinées. Sans mécanismes et incitations fortes à la collaboration au sein de la communauté de la recherche, il existe un risque que ces défis soient abordés de manière déconnectée et cloisonnée, conduisant à gaspiller des ressources limitées et à passer à côté d'opportunités de réaliser de plus grandes économies d'échelle.

Les plateformes peuvent également invoquer délibérément des préoccupations d'ordre juridique ou éthique, telles que la protection des données ou les droits des utilisateurs à la vie privée, pour étouffer la recherche externe et ce, dans certains cas, alors même que les utilisateurs ont activement consenti à partager et à utiliser leurs données à des fins de recherche spécifiques et limitées.[62] Une telle réponse de la part des plateformes, en plus des conditions d'utilisation qui sont floues ou explicitement restrictives pour la recherche d'intérêt public, peut créer un ensemble d'incitations perverses et problématiques pour les chercheurs en ce qui concerne l'équilibrage ou l'atténuation des différents risques juridiques et éthiques. Par exemple, il peut y avoir des cas où des moyens technologiques existent pour collecter des données à partir d'une plateforme (par exemple, des API tierces, des scrapers – des logiciels de téléchargement de données – ou des plug-ins pour la collecte participative de données), mais leur utilisation est interdite par les conditions d'utilisation de la plateforme. Cela peut encourager les chercheurs à employer des moyens trompeurs pour se connecter à une plateforme, une approche douteuse d'un point de vue éthique si la plateforme ou les utilisateurs ne peuvent pas consentir à la participation à la recherche.

Dans de tels cas, la tromperie peut en réalité servir à réduire les risques juridiques pour les chercheurs utilisant ces méthodes ou outils : si les plateformes ou les utilisateurs ne sont pas conscients de la collecte de données en cours, alors la probabilité que les chercheurs soient confrontés à une action en justice est considérablement réduite. L'utilisation de telles méthodes peut également dissuader les chercheurs de publier leurs travaux ou les obliger à être vagues sur les méthodes et outils qu'ils ont utilisés lorsqu'ils les publient. Ceci a à son tour un impact négatif sur la qualité, la comparabilité et la reproductibilité de la recherche en ligne sur des problèmes clés de société. Cela peut aussi engendrer une plus grande méfiance entre les plateformes et la communauté de la recherche au sens large.

Dans l'ensemble, il est urgent de disposer d'un ensemble de normes de base cohérentes pour l'accès des chercheurs aux données des plateformes, à la fois en termes de données auxquelles les chercheurs sont autorisés à accéder et sur la manière dont ils peuvent y accéder. Cela est particulièrement le cas pour la recherche sur les nouvelles plateformes en ligne ou émergentes. De telles normes contribueraient à équilibrer les rapports de force et à réduire les asymétries actuelles entre les plateformes et les chercheurs.

Contexte réglementaire

En dehors de ce projet, nous avons également rencontré des défis similaires dans la conduite de recherches sur une série d'autres plateformes émergentes dans cet écosystème en ligne en constante évolution.[63] Comme l'exercice de cadrage de la plateforme que nous avons mené lors de la phase initiale de ce projet l'a démontré, il existe une large gamme d'autres plateformes en ligne de taille petite et moyenne qui sont également adoptées par des extrémistes et d'autres acteurs nuisibles. Nous craignons que cette tendance ne fasse que s'accroître si les plus grandes plateformes deviennent moins accueillantes pour ces types de communautés et d'activités en ligne, en particulier avec l'entrée en vigueur de réglementations telles que le règlement européen sur les services numériques (DSA).[64] Il est également possible que, au moins à court terme et/ou dans les pays dépourvus de réglementation exigeant l'accès aux données, certaines plateformes puissent chercher à restreindre davantage ou à revenir sur les options d'accès aux données existantes. En l'absence d'exigences réglementaires fortes en matière d'accès aux données, les plateformes pourraient être incitées à éviter le contrôle que peut apporter la recherche indépendante ou à tirer profit de l'accès aux données permis. Par exemple, en février 2023, Twitter a annoncé des changements limitant l'accès gratuit à l'API de Twitter, et il a été rapporté que Meta prévoyait de fermer l'accès aux données existant via CrowdTangle, qui appartient à Meta.[65]

Alors que de nombreux projets de réglementation se concentrent principalement sur les plateformes les plus grandes et les plus dominantes, les changements dans l'environnement réglementaire pour les plateformes en ligne peuvent toujours avoir un impact sur les plateformes en ligne de taille petite et moyenne, bien que dans une moindre mesure. Selon les pays, ces plateformes peuvent toujours être tenues de fournir des conditions d'utilisation plus complètes et cohérentes, une transparence supplémentaire et/ou un meilleur accès aux données pour les régulateurs ou les chercheurs tiers. Les plateformes peuvent également devoir disposer de systèmes permettant de traiter rapidement et efficacement les signalements de contenus ou d'activités illégales sur leurs plateformes. Dans le cas de Telegram, sa croissance considérable ces dernières années pourrait bientôt la soumettre aux mêmes exigences que d'autres

plateformes de grande taille plus établies, dont la conformité nécessiterait des changements significatifs dans son fonctionnement actuel. Dans les années à venir, si les plateformes de taille moyenne comme Discord continuent à se développer, elles pourraient également être confrontées à des obligations réglementaires supplémentaires nécessitant des investissements plus importants en matière de modération des contenus, de transparence et d'accès aux données.

Des plateformes plus petites comme Odysee, qui se sont positionnées comme des alternatives « pro-liberté d'expression » aux grandes entreprises technologiques plus traditionnelles, sont également susceptibles de faire face à un choix : si elles veulent grandir et viser la rentabilité à long terme, elles devront probablement faire face à des exigences réglementaires et à un contrôle plus strict, de même qu'elles auront besoin de ressources techniques et humaines supplémentaires pour garantir que leur plateforme peut gérer une activité accrue. Cependant, cela peut ne pas être populaire auprès de leurs utilisateurs actuels, qui choisissent souvent de rejoindre ces plateformes précisément à cause de leurs approches laxistes en matière de modération de contenu. En revanche, si elles cherchent à apaiser ces types d'utilisateurs ou de communautés en refusant de se conformer aux exigences réglementaires ou juridiques, elles pourraient ne plus être en mesure d'opérer dans certains pays et/ou elles pourraient faire l'objet de poursuites en justice ou de sanctions financières de la part des régulateurs cherchant à freiner les niveaux de contenus ou de comportements préjudiciables que ces plateformes facilitent.

L'examen des dispositions en matière d'accès aux données et des seuils d'utilisateurs dans certaines régulations existantes ou proposées dans des pays clés suggère que bon nombre des problèmes soulevés dans ce rapport ne seront pas entièrement résolus. Une grande partie de la réglementation repose sur les « utilisateurs actifs mensuels » (MAU, pour « monthly active users ») comme indicateur clé pour déterminer si les plateformes atteignent le seuil pour l'ensemble des exigences réglementaires les plus strictes. Cela signifie que de nombreuses plateformes plus petites qui présentent néanmoins des risques en ligne significatifs ne seraient pas tenues d'apporter des solutions aux obstacles existants à l'accès aux données. La section suivante donne un aperçu initial de la réglementation existante ou proposée dans des pays clés, et évalue brièvement si ces différentes réglementations sont susceptibles d'avoir un impact sur les obstacles à la recherche que présentent les plateformes en ligne de taille petite et moyenne. La phase finale de ce projet examinera en détail les implications politiques des défis en matière d'accès aux données que nos recherches ont identifiées.

Union européenne : le Digital Services Act (DSA) et le code de bonnes pratiques renforcé contre la désinformation

Selon le règlement européen sur les services numériques (DSA) de l'UE adopté en juillet 2022, les plateformes seront désignées comme des « très grandes plateformes en ligne » (ou VLOP) si elles ont en moyenne 45 millions d'utilisateurs actifs mensuels (MAU) ou plus dans les pays de l'UE. Ces très grandes plateformes devront fournir un accès en temps réel aux données lorsque cela est techniquement possible, à condition que les données soient accessibles au public (article 40). Cela pourrait inclure des données telles que les interactions agrégées avec le contenu de pages publiques, de groupes publics ou de personnalités publiques, y compris les données relatives aux impressions et aux échanges, telles que le nombre de réactions, de partages et de commentaires. L'accès devrait être fourni dans un délai raisonnable sur demande du régulateur national, le coordinateur pour les services numériques (DSC), du pays de l'UE dans lequel l'entreprise est établie ou de Commission européenne (CE). Les DSC et la Commission européenne ne peuvent utiliser les données fournies que pour surveiller et évaluer la conformité avec le règlement DSA, et ils doivent tenir compte des droits et des intérêts des fournisseurs et des utilisateurs, y compris la protection des données personnelles, des informations confidentielles (les secrets d'affaires) et le maintien de la sécurité du service. Les données devraient être fournies par le biais d'interfaces appropriées spécifiées dans les demandes des DSC ou de la Commission européenne, y compris des bases de données en ligne ou des API.

De même, si le DSC le demande, les données peuvent être fournies à des chercheurs agréés pour contribuer à la détection, au recensement et à la compréhension des risques systémiques identifiés dans le règlement DSA dans l'UE. Les chercheurs agréés doivent être affiliés à une organisation de recherche, être indépendants des intérêts

commerciaux et être en mesure de respecter certaines normes de protection et de sécurité des données. Les chercheurs devront démontrer la nécessité et la proportionnalité de leurs demandes d'accès aux données, rendre public leur financement et rendre tous travaux de recherche disponibles de façon libre et publique. Les prochains actes délégués (législation secondaire de l'UE) introduiront des conditions, des procédures et des mécanismes consultatifs indépendants supplémentaires pour soutenir le partage des données avec les chercheurs externes. Les plateformes devront anonymiser ou pseudonymiser les données à caractère personnel, sauf dans les cas où cela rendrait impossible l'objectif (légitime) de recherche poursuivi.

En 2022, l'UE a également introduit un nouveau code de bonnes pratiques renforcé contre la désinformation (Strengthened Code of Practice on Disinformation), un code volontaire avec actuellement 34 signataires, dont tout un groupe d'organisations intéressées par la lutte contre la désinformation et de grandes entreprises technologiques comme Meta (Facebook et Instagram), Google (YouTube), Twitter, TikTok, Microsoft et Twitch, ainsi qu'un certain nombre de petites entreprises, telles que Clubhouse et Vimeo.[66] Dans la section IV intitulée « Renforcer la communauté de la recherche » (« Empowering the Research Community »), le code contient une série de dispositions relatives à l'accès aux données, dont l'engagement 26 pour que les plateformes signataires fournissent des données non personnelles et des données anonymisées, agrégées ou publiques à des fins de recherche sur la désinformation. Comme pour le règlement DSA, les plateformes devraient fournir un accès aux données en temps réel (ou quasi réel) et lisible par machine via des API ou d'autres mécanismes techniques en licence libre et accessibles, ainsi que s'assurer que des outils et des processus raisonnables soient en place pour atténuer les risques d'abus (tels que des utilisations malveillantes ou à des fins commerciales des données). Pour être éligible, la recherche proposée doit être conforme aux meilleures pratiques éthiques et méthodologiques, par exemple, celles contenues dans le projet de code de conduite sur l'accès aux données des plateformes (Code of Conduct on Access to Platform Data), de l'Observatoire européen des médias numériques (EDMO), et les équipes de recherche peuvent inclure des organisations de la société civile ainsi que des organisations universitaires.[67] Le code de bonnes pratiques renforcé contre la désinformation inclut également l'engagement 27 de créer un organisme tiers indépendant pour évaluer les chercheurs et les projets de recherche.

Parmi les plateformes évaluées dans ce rapport, aucune n'est susceptible d'atteindre le seuil requis par le règlement DSA pour que ces exigences s'appliquent.[viii] En conséquence, bien que les exigences du règlement DSA contribueraient grandement à surmonter les obstacles actuels à la recherche sur les grandes plateformes, elles pourraient ne pas aider à résoudre de nombreux défis décrits dans ce rapport liés à des plateformes de petite ou moyenne taille. De même, aucune des plateformes faisant l'objet de ce rapport n'est actuellement partie au code de bonnes pratiques renforcé contre la désinformation, ce qui signifie que ce code ne résoudra pas non plus les obstacles à la recherche sur des plateformes de petite et moyenne taille telles que Telegram, Discord ou Odysee à moins qu'elles ne s'engagent à respecter ses dispositions.

États-Unis : le Platform Transparency and Accountability Act (PATA) et le Digital Services Oversight and Safety Act (DSOSA)

De manière similaire au règlement DSA, la législation proposée aux États-Unis telle que le Platform Transparency and Accountability Act (loi sur la transparence et la responsabilité des plateformes, PATA)[ix] et le Digital Services Oversight and Safety Act (loi sur la surveillance et la sécurité des services numériques, DSOSA)[x] contiennent tous deux des seuils d'utilisateurs actifs mensuels (MAU) pour déterminer les obligations des plateformes de différentes tailles. Selon la loi PATA, les plateformes hébergeant du contenu généré par les utilisateurs devraient avoir au moins 25 millions de MAU aux États-Unis pour y être soumises (article 2). La législation exigerait que la National Science Foundation (Fondation nationale pour la science, NSF) identifie les données et informations que les plateformes doivent mettre à disposition des chercheurs agréés. Ces informations doivent pouvoir être mises à disposition par

viii Avec environ 38,5 millions d'utilisateurs, Telegram prétend en avoir moins que le seuil de 45 millions pour les VLOP dans l'UE. « FAQ », Telegram, https://telegram.org/faq.

ix PATA – le texte du projet de loi est disponible ici. Un résumé article par article du projet de loi est disponible ici.

x DSOSA – le texte du projet de loi est disponible ici. Un résumé article par article du projet de loi est disponible ici.

les plateformes, proportionnées aux besoins des chercheurs pour réaliser les travaux de recherche et ne pas créer de charges excessives pour la plateforme (article 4). Selon la loi PATA, les chercheurs agréés doivent être affiliés à une université et soumettre des demandes à la NSF pour chaque projet de recherche (article 2). La NSF établirait également un processus pour solliciter des demandes de projets de recherche de la part des chercheurs et définirait des lignes directrices et des critères pour déterminer comment évaluer ces demandes (article 4).

Le projet de loi créerait également un Bureau de la responsabilité et de la transparence des plateformes (Platform Accountability et Transparency Office, PATO) au sein de la Commission fédérale du commerce (Federal Trade Commission, FTC) pour informer les plateformes des demandes de recherche et établir des garanties de confidentialité et de cybersécurité pour l'utilisation des données en question, telles que le chiffrement ou l'anonymisation des données pour protéger la confidentialité des utilisateurs individuels (article 4). Les chercheurs seraient tenus de soumettre une version de leurs recherches avant publication à la plateforme et au PATO pour évaluation afin de confirmer que l'analyse ne divulgue pas d'informations personnelles, de secrets d'affaires ou d'informations commerciales confidentielles (article 5). La loi PATA offrirait également une protection aux chercheurs par la création d'un « refuge sûr » pour empêcher les plateformes de prendre des mesures juridiques contre les chercheurs qui obtiennent des informations de manière consensuelle et avec d'autres mesures de protection de la vie privée en place (article 11). Enfin, le projet de loi permettrait également à la FTC d'exiger que des moyens de signalement ou de divulgation publique soient mis à disposition sous une forme accessible et compréhensible par le public ou accessible pour analyse par les chercheurs, les journalistes et le public à l'aide de mécanismes tels que les API. Cela pourrait inclure les bibliothèques publicitaires, les informations sur les contenus largement diffusés, les informations sur les décisions de modération du contenu ou les informations sur les algorithmes (article 12).

La loi DSOSA, inspirée en partie du règlement DSA de l'UE, fixe le seuil pour les « grandes plateformes couvertes » à 66 millions de MAU et à 10 millions pour les « plateformes couvertes ». Comme pour la PATA, le projet de loi exigerait que la FTC prenne des règles concernant les types de données qui devraient être mis à disposition des chercheurs agréés (article 10, paragraphe c)), y compris les types et les mécanismes d'accès aux données, par exemple en tenant compte de la taille et des techniques d'échantillonnage utilisées pour créer les ensembles de données. La loi exigerait également que les grandes plateformes couvertes fournissent une bibliothèque publicitaire détaillée (article 10, paragraphe f)), un accès à des données clés pour le contenu public à forte portée et à fort engagement, et d'être transparentes sur le contenu qu'elles amplifient (article 10, paragraphe g)). La FTC pourrait choisir de parrainer un Centre de recherche et de développement fédéral (Federally Funded Research and Development Center ou FFRDC) pour faciliter le partage d'informations entre les plateformes couvertes et les chercheurs certifiés. La FTC serait également tenue de garantir que l'accès aux données ne porte pas atteinte aux attentes raisonnables en matière de vie privée des utilisateurs (par exemple en exigeant des plateformes qu'elles anonymisent toute information qui n'est pas du contenu public) et de dire à partir de quand des techniques préservant la vie privée, telles que la confidentialité différentielle et le bruit statistique, devraient être utilisées (article 10, paragraphe c)).

Le projet de loi créerait également un Bureau d'aide à la recherche indépendante (Office of Independent Research Facilitation) au sein de la FTC qui agréerait les chercheurs universitaires et de la société civile pour étudier l'impact des processus de modération du contenu, des décisions de conception de produits et des algorithmes sur la société, la politique, la propagation de la haine, du harcèlement et de l'extrémisme, la sécurité, la vie privée, et la santé physique et mentale (article 10, paragraphe a)). Pour être éligibles, les organisations de recherche devraient être une institution d'enseignement supérieur ou une organisation à but non lucratif (501(c)(3)) ayant pour mission de développer une meilleure compréhension des impacts des plateformes sur la société, ayant la capacité à la fois de se conformer aux règles pour un accès sécurisé pour les chercheurs et d'utiliser des méthodes scientifiques appropriées, et adoptant des méthodes de recherche d'investigation et qualitatives et des meilleures pratiques (article 10, paragraphe b)). Le projet de loi introduirait également des dispositions de sécurité juridique pour les chercheurs agréés qui créent des comptes uniquement pour un projet de recherche ou collectent des informations fournies à des fins de recherche par un utilisateur (par exemple via une extension ou un plug-in dans un navigateur) lorsque l'utilisateur a donné son consentement éclairé (article 10, paragraphe c)).

Comme avec le règlement DSA dans le contexte de l'UE, les seuils fixés dans ces propositions sont susceptibles d'exclure de nombreuses plateformes de petite taille. Bien que le seuil inférieur de 10 millions pour les « plateformes couvertes » dans la loi DSOSA puisse englober certaines plateformes de taille moyenne, comme Telegram ou Discord, les exigences ayant le plus d'impact en matière d'accès aux données visent les grandes plateformes couvertes. En conséquence, aucune des propositions ne traiterait de manière exhaustive les obstacles à la recherche sur les petites plateformes rencontrés lors de nos travaux pour ce rapport. Il convient également de noter que la probabilité que ces projets de loi fédéraux soient adoptés par le Congrès est faible en raison d'un intérêt exécutif plus grand pour la législation axée sur la confidentialité et la concurrence. Il existe aussi des désaccords partisans sur la voie à suivre pour la régulation des médias sociaux (en dehors de la régulation visant spécifiquement à protéger la sécurité en ligne des enfants, qui est susceptible d'avoir de meilleures perspectives). Cela suggère que les États-Unis pourraient être en retard en matière de réglementation introduisant de nouvelles exigences concernant l'accès aux données par rapport à d'autres pays, au moins à court et moyen terme.

Royaume-Uni : Online Safety Bill (OSB)

L'actuelle proposition de loi sur la sécurité en ligne ou OSB dans sa version de février 2023 manque encore de clarté sur un éventuel futur régime d'accès aux données. L'Office des Communications (Office of Communications, Ofcom), le régulateur désigné, pourrait demander des données aux plateformes et éventuellement les partager avec certaines organisations tierces pour mener des recherches de soutien. Dans les deux ans suivant l'adoption de la législation, l'Ofcom devrait également produire un rapport décrivant comment et dans quelle mesure ceux qui mènent des recherches indépendantes sur la sécurité en ligne sont actuellement en mesure d'obtenir des informations des plateformes réglementées. Le rapport examinerait également les problèmes juridiques et d'autre nature qui limitent actuellement l'accès aux données, ainsi que la question de l'étendue d'un éventuel accès plus large. Après la publication du rapport, l'Ofcom pourrait choisir d'adopter des lignes directrices supplémentaires pour les plateformes réglementées et les chercheurs. En comparaison avec le règlement DSA, l'OSB contient des dispositions relativement faibles et un manque de clarté sur l'accès aux données pour les chercheurs, qui pourraient ne pas être clarifiées avant plusieurs années dans le nouveau régime réglementaire. La question de savoir dans quelle mesure l'OSB remédierait (si tant est qu'elle vînt à y remédier) aux obstacles à l'accès aux données soulevés dans ce rapport sur les grandes, moyennes ou petites plateformes, demeure floue.

Allemagne : la loi sur l'application du droit sur les réseaux (NetzDG)

La loi sur l'application du droit sur les réseaux (Netzwerkdurchsetzungsgesetz, NetzDG), introduite pour la première fois en 2017 puis mise à jour en 2021, est un exemple de la première génération de réglementation numérique plus axée sur le contenu, qui se concentre sur la suppression des contenus illégaux en ligne en Allemagne.[68] Cette loi comporte également un seuil d'utilisateurs à partir duquel les plateformes sont concernées, qui est fixé à deux millions ou plus d'utilisateurs enregistrés en Allemagne. La réglementation comprend diverses dispositions d'accès aux données (article 5a) qui permettent aux chercheurs de demander des informations sur la diffusion et l'engagement avec le contenu qui fait l'objet de plaintes ou de suppressions, ainsi que l'accès aux données utilisées pour former les systèmes automatisés des plateformes pour détecter le contenu illégal. Toutes les données demandées doivent être nécessaires pour mener des recherches scientifiques d'intérêt public (par exemple la recherche sur la nature, l'ampleur, les causes et les effets de la communication publique sur les réseaux sociaux), mais il n'y a par ailleurs aucune restriction sur les types d'organisations ou de chercheurs qui peuvent utiliser ces dispositions.

Cependant, la réglementation permet aux plateformes de récupérer les coûts raisonnables associés à la fourniture de données par demande, jusqu'à concurrence de 5 000 €. Les chercheurs doivent également fournir une description de leur approche de la protection des données, par exemple sur les mesures prises pour empêcher que les données ne soient utilisées à d'autres fins ou sur les mesures techniques et organisationnelles prises pour garantir la sécurité des données. Toutes les données partagées par les plateformes doivent être anonymisées ou pseudonymisées dans la mesure du possible, sauf si cela empêche le but de la recherche. Cependant, les mécanismes précis pour partager les données (par exemple via une API) ne sont pas spécifiés, et les dispositions de la NetzDG relatives à l'accès aux

données n'ont pas été largement utilisées par les chercheurs à ce jour, potentiellement à cause des coûts associés. En conséquence, bien qu'elle existe depuis plusieurs années, la NetzDG n'a pas prouvé son efficacité pour faciliter l'accès aux données pour les chercheurs sur les grandes, moyennes ou petites plateformes.

Recommandations

Sur la base des résultats et des implications pour les chercheurs exposées dans ce rapport, ainsi que du contexte réglementaire plus large exposé ci-dessus, nous présentons ici une série de recommandations à l'intention de toutes les plateformes en ligne, des décideurs politiques et des régulateurs ainsi des chercheurs universitaires et de la société civile afin qu'ils puissent dégager des solutions à l'éventail d'obstacles d'ordres technologique, éthique, juridique et liés à la fragmentation que nous avons rencontrés durant nos recherches.

Nous reconnaissons que certaines de nos recommandations entraîneront un surcroît de travail pour les plateformes, notamment pour les plus petites qui disposent de moins de ressources et de capacités techniques. Toutefois, à l'heure actuelle, les plateformes proposent des fonctionnalités efficaces pour permettre la communication et la coordination des acteurs nuisibles et n'offrent que des fonctionnalités réduites ou médiocres pour les recherches d'intérêt public dans ces espaces. Nous estimons qu'il faut remédier à ce déséquilibre.

Obstacles d'ordre technologique

La recherche dans les espaces en ligne modernes fait face à des défis substantiels en raison de la vitesse et de l'échelle à laquelle le contenu peut être créé. L'incapacité technologique à accéder aux données pertinentes, qu'il s'agisse d'obstacles délibérés, des structures compliquées des plateformes ou de technologies mal documentées, a un impact considérable sur la recherche d'intérêt public, en particulier pour les organisations ayant un accès limité aux capacités techniques. La prolifération de nouvelles technologies comme la blockchain ne fera qu'augmenter cette complexité et limiter davantage la disponibilité des outils techniques et de l'expertise.

- **Les plateformes devraient fournir un accès autorisé aux données (via leurs API par exemple) aux chercheurs tiers menant des travaux de recherche d'intérêt public**. À cela devrait s'ajouter une documentation claire, cohérente et accessible, comprenant des conseils sur les types de données pouvant être collectées et des limites suffisantes à la collecte de données personnelles sensibles pour protéger la vie privée des utilisateurs. Dans la mesure du possible, les plateformes devraient également rationaliser la gamme d'outils qu'elles fournissent directement pour accéder aux données afin de réduire la charge des chercheurs devant utiliser plusieurs outils aux capacités qui se superposent.

- **Les décideurs politiques et les régulateurs devraient exiger de toutes les plateformes un accès aux données qui soit précis, fiable et suffisant pour les travaux de recherche d'intérêt public. Cela inclurait l'éventail plus large des plateformes en ligne de petite et de moyenne taille au lieu de ne se concentrer que sur les plus grandes, comme c'est le cas actuellement**. Cela est essentiel pour mieux comprendre comment les activités en ligne illégales ou préjudiciables sont de plus en plus souvent menées ou coordonnées sur des plateformes de taille petite ou moyenne qui peuvent présenter des risques considérables en dépit de leur taille. Autant que possible, les décideurs politiques des différents pays devraient également travailler entre eux pour assurer la cohérence des exigences en matière d'accès aux données pour les plateformes (ce qui permettrait d'éviter de surcharger les petites entreprises) et aider à élaborer de meilleures pratiques à la fois pour les plateformes et les chercheurs avec le temps.

- **Les chercheurs universitaires et de la société civile devraient partager leurs méthodes ou leurs outils de collecte de données efficaces ainsi que toutes leurs connaissances afin de pouvoir suivre le rythme de la multiplication des plateformes en ligne au sein d'un écosystème en ligne en constante évolution**. Sur les plateformes qui nécessitent une plus grande expertise technique pour accéder aux données, beaucoup de temps peut être passé à explorer et à tester des options potentielles. La communauté de la recherche (et ceux qui les financent) devrait chercher à éviter des approches redondantes ou exclusives. Là où cela est possible, ils devraient plutôt

rechercher des économies d'échelle et réduire les désincitations au partage de méthodes, d'outils et d'approches. Cela pourrait être coordonné par des initiatives intersectorielles, comme la Coalition pour la recherche technologique indépendante (Coalition for Independent Tech Research), ou via des organismes d'accès aux données indépendants naissants, comme ceux proposés par l'EDMO ou la Fondation Carnegie pour la paix internationale (Carnegie Endowment for International Peace, CEIP).[69]

Obstacles liés à la fragmentation

Outre la recommandation spécifique suivante liée aux fonctionnalités de recherche systématique sur les plateformes, les recommandations pour surmonter les obstacles d'ordre technologique énoncées ci-dessus contribueraient également à surmonter les obstacles liés à la fragmentation que nous avons identifiés.

- **Les plateformes devraient fournir un accès à leurs données d'une manière systématique qui permette aux chercheurs d'accéder de manière fiable à des données précises provenant de l'ensemble de leurs espaces publics**, plutôt que de devoir explorer manuellement les plateformes à la recherche d'espaces ou de communautés d'intérêt. Cela permettrait une recherche à plus grande échelle mais aussi plus ciblée, car les chercheurs seraient en mesure d'identifier plus facilement les communautés pertinentes (et donc les données). Les outils pour la recherche systématique, qu'ils soient propres aux plateformes ou tiers, devraient faire preuve de leur fiabilité, de leur couverture et de leur précision, ce qui pourrait être soutenu et évalué, par exemple, à travers des contrôles externes menés par des chercheurs ou éventuellement des régulateurs.

Obstacles d'ordre éthique

L'un des principaux défis soulevés par cette recherche est de savoir comment protéger le droit à la vie privée tout en menant des recherches d'intérêt public sur des communautés et des comportements nuisibles. Malheureusement, il n'existe pas de définition commune des espaces privés, ce qui rend difficile pour les chercheurs de déterminer quels espaces devraient être traités comme étant privés ou publics. Dans le même temps, cette absence de définition commune de ce que devrait être un espace privé permet aux plateformes de limiter la transparence ainsi que l'accès à des espaces qui sont aisément accessibles et que l'on peut considérer comme publics.

Comme nous l'avons déjà souligné, des facteurs tels que la taille, l'objectif, l'accessibilité et la nature des relations entre les utilisateurs d'un canal ou d'une communauté devraient être pris en compte lors de l'évaluation de la nature publique ou privée des espaces.[70] Il y a également un danger que les activités illégales ou préjudiciables en ligne ouvertement menées dans des espaces en ligne désignés comme privés puissent créer une incertitude et affaiblir les arguments en faveur du respect de la vie privée (par exemple via le chiffrement) des espaces en ligne et des moyens de communication réellement privés.

- **Les plateformes devraient déterminer une limite raisonnable pour le nombre de membres pouvant participer à des groupes ou à des canaux et déclarer publics les espaces en ligne dont le nombre de membres dépasserait un certain seuil**. Cela devrait également permettre de fournir une plus grande clarté à la fois aux utilisateurs de la plateforme et aux chercheurs tiers sur ce qui est acceptable dans ces espaces, ainsi que sur les types de données qui peuvent être accessibles à des tiers avec des garanties appropriées en matière de protection de la vie privée et des données. Les contenus pour lesquels il n'existe pas d'attentes raisonnables en matière de respect de la vie privée (les contenus postés par exemple sur des pages publiques) devraient être rendus disponibles par l'intermédiaire d'un accès contrôlé à l'API, y compris les données pertinentes sur la portée, les impressions et l'engagement.

- **Si les plateformes étaient réticentes ou peu enclines à le faire volontairement, les décideurs politiques devraient envisager d'exiger des plateformes qu'elles clarifient quels espaces sont véritablement publics ou privés et qu'elles établissent des seuils raisonnables quant au nombre d'utilisateurs pouvant participer à des espaces en ligne privés**. Plutôt que d'introduire des seuils réglementaires généraux dans ce domaine, la réglementation pourrait exiger des entreprises qu'elles fixent des limites claires et raisonnables en fonction

de la nature de leurs plateformes et des évaluations des risques qui tiennent compte des caractéristiques ou des fonctionnalités spécifiques des plateformes (par exemple le chiffrement), des risques et des vulnérabilités potentielles. La réglementation pourrait également encourager les entreprises à indiquer clairement aux utilisateurs quels aspects de leur plateforme sont plus publics ou plus privés, ainsi que les conséquences pour la vie privée des utilisateurs et l'accès aux données par les chercheurs ou les tiers. Un régulateur indépendant pourrait alors évaluer, sur la base de l'évaluation des risques, si la limite fixée par la plateforme est appropriée et atténue suffisamment les risques ou les dommages identifiés.

- **La communauté des chercheurs devrait travailler à formaliser une approche éthique en matière de recherche en ligne sur les espaces publics, semi-privés et privés. Cette approche serait en adéquation avec la gravité potentielle des risques que ces espaces pourraient poser**. De telles approches doivent équilibrer les droits au respect de la vie privée avec les droits de ceux qui pourraient être négativement impactés si ces espaces, en particulier les plus grands et les moins modérés, restaient hors de portée des chercheurs. Ces efforts devraient s'appuyer sur le domaine existant et bien établi de l'éthique de la recherche sur Internet. La coordination pourrait se faire à travers des initiatives existantes telles que l'Association of Internet Researchers (AoIR) ou les futurs organismes d'accès aux données indépendants mentionnés ci-dessus (l'EDMO, par exemple).[71]

Obstacles d'ordre juridique

- **Les plateformes devraient fournir des conditions d'utilisation claires, non seulement en ce qui concerne les types de contenus et d'activités qu'elles autorisent, mais aussi sur la façon dont elles s'appliquent aux chercheurs accédant aux données. Ces conditions devraient être ensuite appliquées de manière cohérente**. Les conditions d'utilisation devraient permettre une recherche d'intérêt public respectueuse de la vie privée plutôt que de permettre à la plateforme de se protéger efficacement la plateforme du contrôle public. Une plus grande clarté dans les conditions d'utilisation permettrait également de fixer des attentes claires concernant l'utilisation des données collectées par des tiers. Cela fournirait plus de certitude pour les chercheurs et aiderait également les utilisateurs à comprendre comment leurs données sont susceptibles d'être utilisées.

- **Les décideurs politiques devraient mettre en place des protections juridiques pour les chercheurs conduisant des travaux de recherche en ligne d'intérêt public et respectueux de la vie privée**. Lorsque les chercheurs utilisent des méthodes et des approches proportionnées et font des efforts suffisants pour protéger la vie privée des utilisateurs, ils ne devraient pas faire face au risque potentiel d'action en justice de la part des plateformes lorsqu'ils étudient des questions sociétales importantes concernant l'ampleur et l'impact des activités illégales ou préjudiciables dans les espaces publics en ligne. Cela est particulièrement pertinent lorsque les conditions d'utilisation de la plateforme sont incomplètes, floues ou ambiguës. Les plateformes ne devraient pas pouvoir échapper complètement aux contrôles en interdisant l'accès aux données dans leurs conditions d'utilisation. En l'absence d'introduction de protections juridiques pour les chercheurs par les gouvernements, les plateformes responsables devraient établir des dérogations volontaires dans leurs conditions d'utilisation pour permettre la recherche au moyen de méthodes comme la collecte de données participative (lorsque les chercheurs ont obtenu le consentement éclairé des utilisateurs).

- **Les chercheurs universitaires et de la société civile devraient également envisager les possibilités de partager ou de mettre en commun leur expertise sur les implications juridiques de l'accès aux données des plateformes**. L'examen juridique des conditions d'utilisation des plateformes et des autres conditions ou politiques connexes peut être long, nécessite beaucoup de ressources et est souvent spécifique aux différents pays d'un point de vue juridique. Étant donné que de nombreux chercheurs n'ont peut-être pas accès à une aide juridique externe (couvrant la protection des données et le droit des contrats), une plus grande coordination et un plus grand partage des ressources et de l'expertise pourraient aider à réduire les risques juridiques et les obstacles à la conduite de travaux de recherche en ligne, et augmenter ainsi l'équité entre les chercheurs. Encore une fois, comme pour les recommandations d'ordre technologique et éthique ci-dessus, ce type de coopération intersectorielle devrait être facilité par les initiatives existantes lorsque cela est possible.

Perspectives

Dans l'ensemble, les perspectives actuelles d'accès des chercheurs aux données des plateformes au sein de l'écosystème en ligne en constante évolution sont mitigées. Bien que la réglementation existante et à venir dans des pays clés offre une promesse considérable en termes d'accroissement de la transparence des plateformes et d'élargissement de l'accès externe aux données, en particulier pour les plus grandes plateformes, comme nous l'avons noté, il existe également des incitations pour les plateformes à ne pas fournir ou à restreindre encore davantage l'accès aux données dans de nombreux contextes. Il reste à voir si les réglementations dans des juridictions clés comme l'UE auront des retombées bénéfiques et si les plateformes décideront d'étendre un accès similaire dans des contextes où elles ne sont pas légalement tenues de le faire.

Une grande partie de cette réglementation n'améliorera pas substantiellement le statu quo concernant de nombreuses plateformes de petite ou moyenne taille qui ne seront pas soumises aux exigences d'accès aux données plus étendues. Cela entraînera probablement une continuation du désemparement des chercheurs face à de nombreuses plateformes, sans aucune garantie que cette situation ne se détériorera pas. Par exemple, certaines entreprises pourraient tenter de restreindre l'accès aux données par des moyens technologiques ou juridiques afin d'éviter un examen réglementaire ou indépendant supplémentaire sur les risques et les contenus ou comportements préjudiciables présents sur leurs plateformes. Indépendamment du fait que les perspectives d'accès aux données puissent s'améliorer, l'écosystème en ligne continuera inévitablement à évoluer à un rythme soutenu, augmentant le nombre, la diversité et la complexité des plateformes en ligne auxquelles les chercheurs pourront souhaiter accéder.

Pour progresser au-delà de la situation actuelle, a minima, les décideurs politiques devraient envisager d'introduire des dérogations ou des protections juridiques pour les chercheurs menant des recherches en ligne d'intérêt public et respectueuses de la vie privée. Les décideurs politiques pourraient également réfléchir à la façon d'inciter et de soutenir davantage les plateformes, par des moyens non réglementaires, à fournir volontairement des outils offrant des données structurées et précises, surtout pour les plateformes qui ne répondent pas aux seuils réglementaires exigeant un plus grand accès aux données. Dans un scénario plus ambitieux qui réduirait considérablement les obstacles à la recherche et qui pourrait nécessiter une réglementation supplémentaire dans de nombreux contextes, les plateformes fourniraient aux chercheurs un accès aux données autorisé, standardisé et respectueux de la vie privée, avec des normes minimales garanties de précision et des conditions d'utilisation claires autorisant la recherche d'intérêt public. Les petites plateformes pourraient avoir besoin d'être soutenues par des ressources pour leur faciliter cette tâche, parallèlement au développement d'un organisme intermédiaire reconnu qui puisse assurer la qualité continue des données et les rendre disponibles de manière standardisée et respectueuse de la vie privée aux chercheurs. Les chercheurs, ainsi que les financeurs de la recherche en ligne, devraient également réfléchir à la façon de créer des économies d'échelle plus importantes dans ce domaine. Cela réduirait les obstacles actuels à la conduite de travaux de recherche qui ralentissent les progrès vers une communauté de recherche plus équitable, diversifiée et mondiale.

Endnotes

1 Guhl, Jakob, Marsh, Oliver et Tuck, Henry, « Recherche sur les évolutions de l'écosystème en ligne : obstacles, méthodes et défis pour l'avenir », Institut pour le dialogue stratégique, avril 2023, https://www.isdglobal.org/isd-publications/recherche-sur-les-evolutions-de-lecosysteme-en-ligne-obstacles-methodes-et-defis-pour-lavenir/.

2 « Extracts From ISD's Submitted Response to the UK Government Online Harms White Paper » [Extraits de la réponse de l'Institut pour le dialogue stratégique au livre blanc du gouvernement britannique sur les préjudices en ligne], Institute for Strategic Dialogue, juillet 2019, https://www.isdglobal.org/isd-publications/extracts-from-isds-submitted-response-to-the-uk-government-online-harms-white-paper/.

3 FAQ pour les canaux, Telegram, https://telegram.org/faq_channels

4 « 700 Million Users and Telegram Premium » [700 millions d'utilisateurs et Telegram Premium], Telegram, juin 2022, https://telegram.org/blog/700-million-et-premium.

5 « Terms of Service » [Conditions d'utilisation du service], Telegram https://telegram.org/tos.

6 « Europol and Telegram take terrorist propaganda online » [Europol et Telegram s'emparent de la propagande terroriste en ligne], Europol, novembre 2019, https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online.

7 Gerster, Lea et al, « Stützpfeiler Telegram. Wie Rechtsextreme und Verschwörungsideolog:innen auf Telegram ihre Infrastruktur ausbauen » [Le pilier Telegram. Comment l'extrême droite et les idéologues du complot développent leur infrastructure sur Telegram], Institute for Strategic Dialogue, décembre 2021, https://www.isdglobal.org/isd-publications/stutzpfeiler-telegram-wie-rechtsextreme-und-verschworungsideologinnen-auf-telegram-ihre-infrastruktur-ausbauen/.

8 « FAQ – Q: What's the difference between groups and channels? » [Quelle est la différence entre les groupes et les canaux ?], Telegram, https://telegram.org/faq#q-what-39s-the-difference-between-groups-and-channels.

9 « Ratings of Telegram groups » [Classement des groupes Telegram], TGStat, https://tgstat.com/ratings/chats.

10 « Belarus Carries Out Wave Of Detentions For Subscribing to "Extremist" Telegram Channels » [La Biélorussie procède à des vagues d'interpellations pour avoir souscrit à des canaux Telegram "extrémistes"], Radio Free Europe/Radio Liberty, octobre 2021, https://www.rferl.org/a/belarus-telegram-extremist-detentions/31530720.html.

11 « Через сервис TGStat стали доступны данные о протестных приватных чатах и их участниках » [Des données sur des chats privés d'opposition et leurs utilisateurs devenues publiques à cause du service TGStat], Mediazona, avril 2022, https://mediazona.by/news/2022/04/28/tgstat.

12 Frühling, Milla, « OLIVER JANICH – QANON-DESINFORMATIONEN AUF ALLEN KANÄLEN » [Le mouvement conspirationniste QAnon d'Oliver Janich présent sur tous les canaux], Belltower.News, octobre 2020, https://www.belltower.news/social-media-rechtsaussen-oliver-janich-qanon-desinformationen-auf-allen-kanaelen-105577/.

13 « TELEGRAM-KANAL », Oliver Janich Investigativ, https://www.oliverjanich.de/telegram-messenger.

14 Institute for Strategic Dialogue, juillet 2019, op. cit.

15 Gerster et al, décembre 2022, op. cit.

16 Rogers, Iain, « Germany Foils Plot to Sabotage Democracy, Kidnap Health Minister » [L'Allemagne déjoue un complot visant à saboter la démocratie et à kidnapper le ministre de la santé], Bloomberg UK, avril 2022, https://www.bloomberg.com/news/articles/2022-04-14/germany-foils-plot-to-sabotage-democracy-kidnap-health-minister.

17 « Razzia wegen Mordplänen gegen Kretschmer » [Descente de police suite à des projets d'assassinat contre Kretschmer], ZDFheute, décembre 2021, https://www.zdf.de/nachrichten/politik/razzia-telegram-mordplan-kretschmer-100.html.

18 « Täglich Tötungsaufrufe auf Telegram » [Appels au meurtre quotidiens sur Telegram], Tagesschau, January 2021, https://www.tagesschau.de/investigativ/funk/ todesdrohungen-telegram-101.html.

19 « Ermittler decken illegalen Handel auf » [Les enquêteurs mettent au jour un commerce illégal], Tagesschau, octobre 2020, https://www.tagesschau.de/inland/telegram-illegaler-handel-105.html.

20 Voir par exemple : Sold, Manjana et Junk, Julian, « Researching Extremist Content on Social Media Platforms: Data Protection and Research Ethics Challenges and Opportunities » [La recherche de contenus extrémistes sur les plateformes de médias sociaux : défis et opportunités d'ordre éthique en matière de protection des données et de recherche], Global Network on Extremism and Technology, 2021, https://gnet-research.org/wp-content/uploads/2021/01/GNET-Report-Researching-Extremist-Content-Social-Media-Ethics.pdf; Conway, Maura, « Online Extremism and Terrorism Research Ethics: Researcher Safety, Informed Consent, et the Need for Tailored Guidelines, Terrorism and Political Violence » [Éthique de la recherche en ligne sur l'extrémisme et le terrorisme : sécurité des chercheurs, consentement éclairé et besoin de règles appropriées, terrorisme et violence politique], Terrorism and Political Violence, 33 (2), pp. 367–380, mars 2021, 10.1080/09546553.2021.1880235; « Internet Research: Ethical Guidelines 3.0 » [Recherche en ligne : lignes directrices en matière d'éthique 3.0], AoIR, octobre 2019, https://aoir.org/reports /ethics3.pdf; « A Guide to Internet Research Ethics » [Guide sur l'éthique dans la recherche en ligne], NESH, juin 2019 https://www.forskningsetikk.no/en/guidelines/social-sciences-humanities-law-and-theology/a-guide-to-internet-research-ethics/.

21 « PROJEKT RADIKALISIERUNG IN RECHTSEXTREMEN ONLINE-SUBKULTUREN ENTGEGENTRETEN » [Projet de lutte contre la radicalisation dans les sous-cultures d'extrême droite en ligne], Institute for Strategic Dialogue Germany, https://isdgermany.org/projekt-bmj/.

22 « Nazi-Song ist Antifa-Experiment » [La chanson nazie est une expérimentation des antifas], Taz, janvier 2022, https://taz.de/Rechte-Musik-auf-Streaming-Plattformen/!5828978/.

23 Dockery, Wesley, « Germany cracks down on far-right Telegram users » [L'Allemagne sévit contre les utilisateurs de Telegram d'extrême droite], Deutsche Welle, septembre 2022, https://www.dw.com/en/germany-cracks-down-on-far-right-telegram-users/a-60715438.

24 « FAQ – Q: There's illegal content on Telegram. How do I take it down? » [Il y a du contenu illégal sur Telegram. Comment puis-je le faire retirer ?], Telegram,

https://telegram.org/faq#q-there-39s-illegal-content-on-telegram-how-do-i-take-it-down.

25 « Antwort der Landesregierung auf eine Kleine Anfrage zur schriftlichen Beantwortung » [Réponse du gouvernement du Land à une petite question pour réponse écrite], Landtag Von Sachsen-Anhalt, https://www.landtag.sachsen-anhalt.de/fileadmin/files/drs/wp8/drs/d1519aak.pdf.

26 Efforts to delegitimise the state [Efforts de délégitimation de l'État], Bundesamt für Verfassungsschutz, https://www.verfassungsschutz.de/EN/topics/efforts-to-delegitimise-the-state/efforts-to-delegitimise-the-state_node.html

27 « Mit Haftbefehl gesuchter Hetzer Attila Hildmann sieht sich als Nachfolger von Adolf Hitler » [Attila Hildmann, l'agitateur recherché par un mandat d'arrêt, se voit comme le successeur d'Adolf Hitler], RTL, octobre 2022, https://www.rtl.de/cms/attila-hildmann-von-stern-reportern-in-der-tuerkei-aufgespuert-er-wird-mit-haftbefehl-gesucht-5013127.html.

28 Steinke, Ronen, « Verfassungsschutz : Allein unter falschen Freunden » [L'office de protection de la constitution : seul parmi de faux amis], Süddeutsche Zeitung, septembre 2022, https://www.sueddeutsche.de/projekte/artikel/politik/verfassungsschutz-rechtsextreme-social-media-telegram-virtuelle-agenten-reichsbuerger-coronaleugner-rassismus-antisemitismus-verschwoerungsideologie-e222942/?reduced=true.

29 Curry, David, « Discord Revenue and Usage Statistics (2023) » [Statistiques sur les recettes et les utilisations de Discord], Business of Apps, janvier 2023, https://www.businessofapps.com/data/discord-statistics/.

30 « Top 100 Biggest Discord Servers » [Le top 100 des plus gros serveurs Discord], Discord, https://discords.com/servers/top-100.

31 « Discord servers tagged with 4Chan » [Serveurs Discord « étiquetés » 4chan], Disboard, https://disboard.org/servers/tag/4chan.

32 Roose, Kevin, « This Was the Alt-Right's Favorite Chat App. Then Came Charlottesville » [C'était l'application préférée de l'Alt-droite américaine, puis sont arrivés les événements de Charlottesville], The New York Times, août 2017, https://www.nytimes.com/2017/08/15/technology/discord-chat-app-alt-right.html; Davey, Jacob, et Ebner, Julia, « The Fringe Insurgency – Connectivity, Convergence et Mainstreaming of the Extreme Right » [Mouvements insurrectionnels périphériques : connectivité, convergence et banalisation de l'extrême droite], Institute for Strategic Dialogue, octobre 2017, https://www.isdglobal.org/isd-publications/the-fringe-insurgency-connectivity-convergence-and-mainstreaming-of-the-extreme-right/.

33 Alexander, Julia, « Discord is purging alt-right, white nationalist and hateful servers » [Discord élimine les serveurs de l'Alt-droite américaine, nationalistes blancs et haineux], Polygon, février 2018, https://www.polygon.com/2018/2/28/17061774/discord-alt-right-atomwaffen-ban-centipede-central-nordic-resistance-movement.

34 Allyn, Bobby, « Group-Chat App Discord Says It Banned More Than 2,000 Extremist Communities » [L'application de messagerie de groupe Discord dit avoir supprimé plus de 2 000 communautés extrémistes], NPR, avril 2021, https://www.npr.org/2021/04/05/983855753/group-chat-app-discord-says-it-banned-more-than-2-000-extremist-communities.

35 Gallagher, Aoife et al, « Gaming and Extremism: The Extreme Right on Discord » [Gaming et extrémisme : l'extrême droite sur Discord], Institute for Strategic Dialogue, août 2021, https://www.isdglobal.org/isd-publications/gaming-and-extremism-the-extreme-right-on-discord/.

36 Ibid.

37 Ayad, Moustafa, « Islamogram: Salafism and Alt-Right Online Subcultures » [« Islamogram » : salafisme et sous-cultures de l'Alt-droite américaine en ligne], Institute for Strategic Dialogue, novembre 2021, https://www.isdglobal.org/isd-publications/islamogram-salafism-and-alt-right-online-subcultures/.

38 Wong, Wilson, « Discord chat app faces moderation questions after mass shooting suspects are linked to platform » [La modération sur l'application de messagerie de groupe Discord en question après avoir découvert que les suspects dans l'affaire de la tuerie de masse étaient liés à la plateforme], NBC News, juillet 2022, https://www.nbcnews.com/tech/tech-news/highland-park-shooting-suspect-bobby-e-crimo-iii-discord-server-raises-rcna36659.

39 Joyce, Kathryn et Lorber, Ben, « «Traditional» Catholics and white nationalist «groypers» forge a new far-right youth movement » [Un nouveau mouvement de jeunesse d'extrême droite créé par des catholiques « traditionnels » et des membres du mouvement nationaliste blanc « Groyper »], Salon, mai 2022, https://www.salon.com/2022/05/13/trad-catholics-and-nationalist-groypers-forge-a-new-far-right-youth-movement/.

40 Disboard, https://disboard.org/.

41 « Channel Resources » [Ressources sur les canaux], Discord, https://discord.com/developers/docs/resources/channel - get-channel-messages; « Dracovian/Discord-Scraper » [Dracovian/Logiciel de téléchargement de données pour Discord], Github (via Internet Archive), https://web.archive.org/web/20220727182403/https://github.com/Dracovian/Discord-Scraper.

42 « Terms of Service » [Conditions d'utilisation du service], Discord, https://discord.com/terms.

43 « Discord Developer Policy » [Politique de Discord à l'égard des développeurs], Discord, https://discord.com/developers/docs/policies-and-agreements/developer-policy. Remarque : La politique de Discord à l'égard des développeurs a été mise à jour en septembre 2022 et prévoit dorénavant ce qui suit à la place de l'ancienne formulation mentionnée dans le texte : « Il est interdit d'extraire ou de récupérer des données, du contenu ou des informations disponibles sur ou via l'intermédiaire des services Discord ».

44 Schlegel, Linda, « Jumanji Extremism? How games and gamification could facilitate radicalization processes » [Extrémisme Jumanji ? Comment les jeux et la gamification peuvent faciliter les processus de radicalisation], Journal for Deradicalization, 23, Été 2020, pp. 1–44.

45 Vogel, William, « People-first video platform Odysee Launches out of Beta, Enabling Creators to Reclaim Power and Monetization » [La plateforme vidéo Odysee, centrée sur l'utilisateur, sort de sa version bêta en permettant aux créateurs de reprendre le pouvoir et la monétisation], Cision PRWeb, avril 2023, https://www.prweb.com/releases/peoplefirstvideoplatformodyseelaunchesoutof-betaenablingcreatorstoreclaim-powerandmonetization/prweb17586549.htm.

46 Odysee (@OdyseeTeam), « La censure des grandes entreprises technologiques est allée trop loin ! Utilisez Odysee comme alternative à YouTube. Nous ne sommes pas parfaits, mais nous nous améliorons. Pour information : Diffusez en direct avec nous et gagnez plus d'argent que sur YouTube/Twitch grâce aux dons », Twitter, 30 septembre 2021, https://twitter.com/OdyseeTeam/status/1443642146280509464.

47 Odysee (@Odysee), « Odysee & Freedom of the Press: A Letter From Our CEO » [Odysee et la liberté de la presse : lettre de notre PDG], Odysee, mars 2022, https://odysee.com/@Odysee:8/freedomofthepress:0.

48 Matlach, Paula, Hammer, Dominik and Schwieter, Christian, « Auf Odysee: Die Rolle von Blockchain-Technologie für die Monetarisierung im rechtsextremen Onlinemilieu » [Le rôle de la technologie de la blockchain dans la monétisation dans les milieux en ligne d'extrême droite : l'exemple d'Odysee], Institute for Strategic Dialogue, août 2022, https://www.isdglobal.org/wp-content/uploads/2022/08/ISD_auf-odyssee_220810_digital.pdf.

49 Odysee (@OdyseeTeam), « Nous ne sommes pas une alt tech [technologie alternative], nous sommes une new tech [nouvelle technologie]. Alt tech = version inférieure de ce qui existait avant sans autre fonds de commerce que la liberté d'expression. New tech = meilleure version de ce qui existait avant avec le bénéfice de la liberté d'expression », Twitter, 3 août 2021, https://twitter.com/OdyseeTeam/status/1422629329905848322.

50 LBRY, https://lbry.com/.

51 « Jeremy Kauffman: Leadership For New Hampshire » [Jeremy Kauffman : un leadership pour le New Hampshire »], https://jeremy4nh.com/home/

52 Matlach, Paula, Hammer, Dominik et Schwieter, Christian, août 2022, op. cit.

53 « New breed of video sites thrive on misinformation and hate » [Un nouveau genre de sites vidéo prospère sur la désinformation et la haine], Rappler, août 2022, https://www.rappler.com/technology/features/new-breed-video-sites-thrive-misinformation-hate/.

54 Marshall, Andrew R. C. et Tanfani, Joseph, « New breed of video sites thrives on misinformation and hate » [Un nouveau genre de sites vidéo prospère sur la désinformation et la haine], Reuters, août 2022, https://www.reuters.com/investigates/special-report/usa-media-misinformation/.

55 « Sign-up » [Rejoindre], Odysee, https://odysee.com/$/signup?redirect=/.

56 Odysee (@Odysee), « Creators Will Be Earning From Ads Soon » [Les créateurs de contenus gagneront bientôt de l'argent grâce aux publicités], Odysee, octobre 2021, https://odysee.com/@Odysee:8/creator-earnings:7.

57 Talley, Ian, « Islamic State Turns to NFTs to Spread Terror Message » [L'État islamique se tourne vers les NFT pour diffuser un message de terreur], The Wall Street Journal, septembre 2022, https://www.wsj.com/articles/islamic-state-turns-to-nfts-to-spread-terror-message-11662292800.

58 « Terms of Service » [Conditions d'utilisation du service], Odysee, https://odysee.com/$/tos.

59 « Les origines de l'extrême droite », herodote.net, octobre 2022, https://www.herodote.net/Les_origines_de_l_extreme_droite-article-2715.php.

60 « Odysee.com », Similar Web (via Internet Archive), https://web.archive.org/web/20221018123152/https://www.similarweb.com/website/odysee.com/; « Youtube.com », Similar Web (via Internet Archive), https://web.archive.org/web/20221018122916/https://www.similarweb.com/website/youtube.com/#overview.

61 « Declaration of Indifference: Community Guidelines » [Déclaration d'indifférence : règles communautaires], Odysee, février 2022, https://help.odysee.tv/communityguidelines/.

62 Voir par exemple : Mir, Rory et Doctorow, Cory « Facebook's Attack on Research is Everyone's Problem » [Les attaques de Facebook sur la recherche sont l'affaire de tous], EFF, août 2021, https://www.eff.org/deeplinks/2021/08/facebooks-attack-research-everyones-problem.

63 Voir par exemple : Hammer, Dominik, Gerster, Lea et Schwieter, Christian, « Inside the Digital Labyrinth: Right-Wing Extremist Strategies of Decentralisation on the Internet & Possible Countermeasures » [Au cœur du labyrinthe numérique : stratégies des extrémistes d'extrême droite et solutions envisageables], Institute for Strategic Dialogue, février 2023, https://www.isdglobal.org/wp-content/uploads/2023/02/Inside-the-Digital-Labyrinth.pdf.

64 « Digital Services Act », Parlement Européen, https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.pdf.

65 « Twitter API Changes Set to Disrupt Public Interest Research » [L'API de Twitter modifiée pour limiter la recherche d'intérêt public], Tech Policy Press, février 2023, https://techpolicy.press/twitter-api-changes-set-to-disrupt-public-interest-research/; Lawler, Richard, « Meta reportedly plans to shut down CrowdTangle, its tool that tracks popular social media posts » [Meta envisagerait de supprimer CrowdTangle, son outil qui permet de suivre les publications populaires sur les réseaux sociaux], The Verge, juin 2023, https://www.theverge.com/2022/6/23/23180357/meta-crowdtangle-shut-down-facebook-misinformation-viral-news-tracker.

66 « Signatories of the 2022 Strengthened Code of Practice on Disinformation » [Signataires du code de bonnes pratiques renforcé contre la désinformation de 2022], Commission Européenne, juin 2022, https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation.

67 « EDMO releases report on researcher access to platform data » [L'EDMO publie un rapport sur l'accès des chercheurs aux données des plateformes], Observatoire européen des médias numériques, mai 2022, https://edmo.eu/2022/05/31/edmo-releases-report-on-researcher-access-to-platform-data/.

68 « Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act, NetzDG) – Basic Information (2017) » [Loi visant à renforcer l'application du droit sur les réseaux sociaux (loi sur l'application du droit sur les réseaux sociaux) : informations essentielles (2017)], Bundesministerium der Justiz, https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html.

69 Coalition for Independent Technology Research, https://independenttechresearch.org/; Observatoire européen des médias numériques, mai 2022, op. cit. ; Wanless, Alicia et Shapiro, Jacob N., « A CERN Model for Studying the Information Environment » [Le modèle du CERN en matière d'étude de l'environnement de l'information], Carnegie Endowment for International Peace, novembre 2022, https://carnegieendowment.org/2022/11/17/cern-model-for-studying-information-environment-pub-88408.

70 Institute for Strategic Dialogue, juillet 2019, op. cit.

71 « Ethics » [Éthique], AoIR, https://aoir.org/ethics/.

ISD | Powering solutions to extremism and polarisation

Copyright © ISD (2023). Institute for Strategic Dialogue (ISD) est une société à responsabilité limitée par garantie, siège social à l'adresse PO Box 75769, Londres, SW1P 9ER. ISD est enregistrée en Angleterre sous le numéro d'enregistrement de société 06581421 et sous le numéro d'enregistrement d'organisme de bienfaisance 1141069. En France, l'ISD est établi sous la forme d'une association Loi 1901 : l'Institut pour le Dialogue Stratégique sous le numéro d'enregistrement W751256497. Tous droits réservés. Toute copie, reproduction ou exploitation de tout ou partie de ce document ou de ses pièces jointes sans l'autorisation écrite préalable d'ISD est interdite.

Amman | Berlin | London | Paris | Washington DC

www.isdglobal.org