

Darknets et Anarchives

Vincent Bonnefille

DANS **AGENCEMENTS** 2024/1 (N° 10), PAGES 164 À 168

ÉDITIONS **ÉDITIONS DU COMMUN**

ISSN 2608-5739

ISBN 9791095630616

DOI 10.3917/agen.o10.o164

Article disponible en ligne à l'adresse

<https://www.cairn.info/revue-agencements-2024-1-page-164.htm>



CAIRN.INFO
MATIÈRES À RÉFLEXION



Découvrir le sommaire de ce numéro, suivre la revue par email, s'abonner...

Flashez ce QR Code pour accéder à la page de ce numéro sur Cairn.info.

Distribution électronique Cairn.info pour Éditions du Commun.

La reproduction ou représentation de cet article, notamment par photocopie, n'est autorisée que dans les limites des conditions générales d'utilisation du site ou, le cas échéant, des conditions générales de la licence souscrite par votre établissement. Toute autre reproduction ou représentation, en tout ou partie, sous quelque forme et de quelque manière que ce soit, est interdite sauf accord préalable et écrit de l'éditeur, en dehors des cas prévus par la législation en vigueur en France. Il est précisé que son stockage dans une base de données est également interdit.

Vincent BONNEFILLE

a vu dans le chiffrement un black bloc envoyé au visage du capitalisme surveillant. Un espace à soi, jamais sans les autres. Depuis, iel milite pour une informatique libératrice et consentie. Sa recherche en accès libre est disponible sur les réseaux.

DARKNETS ET ANARCHIVES

Communément, un « darknet » sert à désigner de façon péjorative une catégorie de protocoles réseau atypiques. Ils rajoutent une couche de sécurité numérique aux connexions, dissimulent l'identité d'origine des machines qui s'y connectent. Les sources, serveurs ou clients, y sont protégées. Ces pairs (nœuds du réseau) sont ainsi plus difficiles à tracer, contrôler ou censurer. En cela, ils portent un certain degré de l'utopie anarchique : celle d'échapper à l'emprise des programmes ennemis et gouvernant. Ils sont souvent le refuge de communautés réprimées ou criminelles, ailleurs interdites d'existence.

L'État français et sa police criminalisent de plus en plus l'usage de ces outils de chiffrement des données, indispensables à la protection de nos espaces de vie numériques. Le Journal Officiel de la République Française du 26 septembre 2017¹ traduit « darknet » (réseau obscur en anglais) par « internet clandestin ». À défaut de pouvoir briser le secret conféré par le chiffrement, la police, devant la justice et les médias, tente de retourner la charge de la preuve (qu'elle n'arrive pas à arracher), faisant du chiffrement des données un acte en soi criminel. Les gouvernements, démunis, ainsi mis à distance, ré-ouvrent le débat originel qui accompagna le basculement des outils de chiffrement dans le domaine public : l'État devrait-il être le seul à même de faire ou de défaire le secret informatique ?

Depuis la crypto-war (d'après guerre) l'informatique mondial a bien changé. Aux débuts d'internet, la population restreinte d'ordinateurs forme des réseaux disparates, dédiés aux activités gouvernementales et universitaires. Ils sont cartographiés grâce à leurs adresses IP (Internet Protocol). Durant cette actualisation, certains ordinateurs pourtant connus, existant sur des réseaux extérieurs, restent muets aux pings qui leur sont envoyés (et auxquels ils sont sensés répondre). Un comportement réfractaire, secret, qui leur vaudra le nom de "Darknets". Cette histoire des origines² s'appuie sur des sources inconsistantes, des hyperliens rompus (qu'Internet Archive n'a pas sauvegardés). Elle nous raconte quelque chose de familier : les projets d'indexation du savoir se heurtent à des limites parfois infranchissables dont les causes restent à déterminer (panne, bug, discontinuité,

1. N° 0225, du 26 septembre 2017 (texte n° 110).

2. Page Wikipédia française relatant cet épisode historique : https://fr.wikipedia.org/wiki/Darknet#cite_note-6

maintenance, etc). À l'époque, l'opacité de ces darknets était sans doute sécuritaire (au fait de vouloir garder privés leurs contenus), mais on pourrait y voir un geste anarchiviste : celui de refuser aux projets d'indexation la capacité de lever le mystère, d'informer les choses pour en tirer un pouvoir stratégique, prédictif.

La catégorie "darknet" sert souvent un récit (*spin*) politique non neutre qui entretient les préjugés à l'endroit de ces réseaux (*networks*) qualifiés de "sombres" (*dark*). La radicalité contre-intuitive des applications de la cryptographie (dont les chiffrements font partie) ainsi que la médiatisation outrancière de ces réseaux autour des marchés noirs et réseaux pédophiles ou de tueurs à gage en font le lieu de fantasmes et récits d'épouvante. On se laisse convaincre que ces protocoles quasi magiques donneraient accès à des ordinateurs quantiques, à des *backrooms* et autres *redrooms*. Entre désir de croire et peur d'y accéder, les récits horribles, ARG et *creepypasta*³ font parfois du darknet un antagoniste techno-effrayant hors de contrôle : figure de l'infocalypse⁴. Tréfonds d'Internet, il tient le rôle de refoulé archivistique, immodéré, dernière demeure des *lostmedias*.

Certaines narrations spéculatives théorisent qu'Internet est déjà mort, en grande majorité peuplé de *bots* et de *scrapers*⁵. Un vocabulaire extractiviste cherche à circonscrire les limites de son art. Les *dark datas* désignent ces amas de données inexploitable par les entreprises. Elles sont inutilisables, mal formées, mal indexées ou encore sorties du champ légal ou sous évaluées. Elles peuvent dater d'un âge sombre du numérique⁶, produites selon des protocoles et des standards aujourd'hui obsolètes. Le *deep web* désigne quant à lui ces parties du web, protégées derrière un mot de passe qui, de fait, échappent aux sondes des moteurs de recherche et à certaines entreprises fouineuses.

Des moteurs de recherche qui nous ont habitués à faire "remonter" l'information sans effort. Une agrégation instantanée qui invisibilise tout un préalable technique. Ici, la « classe vectorialiste »⁷ s'accapare le travail collectif des internautes déjà passés par là. Un web devenu régie publicitaire qui fait tout pour nous garder captives, inféodés⁸ à des services gratuits, sécurisés et modérés (mais capitalistes de nos données). Des plateformes dont le monopole déforme le cyberspace⁹ en faisant graviter toutes les activités vers elles. Heureusement, des alternatives libres existent : un web artisanal, minutieusement agencé, affectivement curaté (*webrings*, annuaires, etc) ; un indie-web entretenu à la marge permettant la dérive retrouvée des débuts du www.

3. *Creepypasta : des récits spaghettis, culture populaire d'épouvante ; ARG pour Alternative Reality Game : des récits mêlant éléments réels et intrigue fictionnelle.*

4. Jacob Appelbaum & Julian Assange & Andy Müller-Maguhn & Jérémie Zimmermann, *Menace sur nos libertés : comment Internet nous espionne, comment résister*, ed. Robert Laffont, 2013, « Les quatre cavaliers de l'Infocalypse : la pornographie enfantine, le terrorisme, le blanchiment d'argent, les guerres de la drogue ».


5. @IlluminatiPirate, *Dead Internet Theory : Most of the Internet is Fake*, janvier, 2021 : <https://forum.agoraroad.com/index.php?threads/dead-internet-theory-most-of-the-internet-is-fake.3011/>

6. Terry Kuny, *A Digital Dark Ages ? Challenges in the Preservation of Electronic Information*, 1998 : <https://archive.ifa.org/IV/ifa63/63kuny1.pdf>, causes d'un une archive obsolète, p. 4-5.

7. McKenzie Wark, *Un manifeste hacker*, Criticalsecret, 2006, partie n°21, oppose la classe vectorialiste en lutte pour déposséder intellectuellement la classe hacker (créatrice).

8. Cédric Durand, *Technoféodalisme : Critique de l'économie numérique*, La Découverte, 2020 : <https://bib.vincent-bonnefille.fr/book/136>

9. Louise Drühle, *L'atlas critique d'Internet : spatialisation d'un objet complexe en vue d'en comprendre les enjeux socio-politiques*, 2014 : <https://louisedrulle.fr/internet-atlas/#Ch8>

10. Joel Hooks,  *My blog is a digital garden*, not a blog.

11. Experiencespoetiques citant le Senslab : <https://experiencespoetiques.wordpress.com/lisiere/anarchive/>, 2018, il s'agit d'une recherche incrémentale, d'un événement à l'autre.

12. Antoinette Rouvroy & Thomas Berns, *Le nouveau pouvoir statistique : ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps « numériques »*, 2010, *Multitudes*, 2010/1 (n° 40).

13. Dorothée Dussy, *Le Berceau des dominations*, Pocket, 2021 : « À la faveur du réel et de la banalité des abus sexuels commis sur les enfants, on verra que l'inceste est structurant de l'ordre social. Il apparaît aussi comme l'outil primal de formation à l'exploitation et à la domination de genre et de classe. »

Des chercheurs·euses ouvrent des jardins digitaux¹⁰, des logs et blogs, qui privilégient le voisinage d'objets rhizomiques : une sorte d'« anarchie » (un mot-valise qui, comme « darknet », s'invente à l'usage). Ces modalités de pratique n'aboutissent pas toutes à un faire anarchique. En revanche, ces protocoles tentent d'échapper au pouvoir disciplinaire qui les bride, les ennuit, limitent le champ de leur art. Faire une anarchie s'apparente à de la recherche-création¹¹ : la multiplication de formes, objets et prototypes, permettant d'avancer dans la résolution d'une problématique commune. Une archive mouvante, transmédia-tique, incrémentée tout le long d'une recherche en cours. Une hiérarchisation du savoir dont l'index informel ouvre des virtualités interprétatives, d'autres cheminements. Il s'agit peut-être aussi de séparer au moins le moment de l'atelier de celui de l'exposition.

On peut aussi penser l'anarchie comme position anti-archivis-tique, allant contre les pouvoirs d'indexation et de catégorisation. Une résistance contre la numérisation du monde, l'extractivisme des données au service d'une surveillance de masse, imposée à nous par sa gouvernementalité algorithmique¹² (douce et sans friction politique).

L'anarchie est aussi une archive produite par des communautés marginales et informelles qui, par le récit commun, se construisent politiquement, se donnent droit au chapitre. Le darkweb – le web dont les sources sont cachées en passant par des protocoles dits « darknets » – forme des espèces d'espaces autres, hétérotopiques, dont le régime de confiance entre anonymes incite ces pairs à inventer d'autres modalités d'existence : leurs propres arts. S'y développent des cultures subalternes et *underground*. Des terrains de recherche faisant rarement archive publique émergent ainsi aux yeux de qui veut les trouver.

Sur certains forums intraquables, des pédocriminels s'échangent des contenus explicites sans crainte apparente. Ces groupes peuvent y défendre des thèses positivantes leurs actes : soutenir que ces pratiques sexuelles sont naturelles, relativiser ces violences avec d'autres elles aussi commises dans le cercle domestique, ou y voir rien de plus que des modalités éducatives (celles du pouvoir patriarcal). La culture du viol, diffuse dès le berceau¹³, institue cette domination comme tolérable et impunie. Une banalisation des violences de classe (sexistes) qui, en s'exposant dans certains coins du web, doit nous rappeler combien celles-ci sont répandues, banales, mais tabous, silencialisées. Des violences dont les

réseaux chiffrés peuvent effectivement être le moyen de diffusion, en aucun cas la cause.

Au regard de ces violences, l'épouvantail de l'infocalypse sert un récit politique diabolisant Internet et les messageries chiffrées rendues monstrueuses. La panique morale sert de levier pour rendre acceptables des projets de surveillance : des lois et logiciels élargissant le champ d'intervention policier et judiciaire. L'installation de portes dérobées et de sondes est présentée comme une solution préventive. De telles insertions logicielles diminueraient le pouvoir d'exclusivité que les applications de communication chiffrée procurent à leurs usagers. Le risque est qu'une fois ces mouchards mis en place, les États-entreprises ciblent des populations stigmatisées pour leur orientation sexuelle ou leur genre, leur origine ethnique ou appartenance religieuse et, bien entendu, leur position politique (jugée militante ou d'opposition). De telles failles, injectées volontairement dans nos espaces de vie privée, induiraient un climat d'incertitude qui affecterait les corps militants et journalistiques. Or, Wikileaks nous l'a montré, une chaîne discontinue du secret peut renverser la symétrie du pouvoir et la fabrication de ses récits.

L'horizon des ordinateurs quantiques ou encore les logiciels espions (Pegasus et consorts) sont d'une sophistication qui à l'instar du chiffrement peut nous sembler appartenir au monde des hackers et du renseignement. Les armes d'infiltration ou de pression politique qui violent le secret des sources et de la correspondance portent atteinte aux métiers journalistiques. Elles ne sont pas le fait de régimes politiques dits autoritaires. Le chiffrement est l'un des moyen défensifs qu'il nous reste en commun pour garantir le droit d'informer et de s'organiser. Nous devons connaître nos propres failles, étudier les stratégies ennemies, les prévenir.

Il nous faut des espaces compétents pour accompagner et croire les victimes de violences et d'abus sexuels ou mentaux. Voir les *reds flags*. De même que les toxicomanes sont poussés vers les marchés noirs, plutôt que de les exclure du champ d'action social et solidaire. Ne pas se laisser penser que le pire est réservé aux autres (qui l'ont bien mérité). Ne pas, essentialiser le pire dans des objets fantasmés d'un lointain réseautique. Dans la noirceur de ces réalités, dans ce vocabulaire guerrier, nous devons nous équiper sans attendre le pire. Parfois, il faut peu de choses pour retrouver un peu de bien-être numérique : des logiciels et systèmes d'exploitation libres sont autant de jardins.

Le darknet est une figure d'épouvante technologique servant par contraste à légitimer l'action surveillante des États-entreprises qui se présentent comme étant les seules garants de la cohésion sociale sécuritaire. Ils pointent du doigt toute pratique du secret qui réduit leur terrain politique d'action, de prévention ou d'influence. Ces empires veulent nous habituer à tout exposer de nos vies en nous disant que nous n'avons rien à cacher. La gouvernamentalité algorithmique se nourrit de ces silos d'information, agit, indolore, pour nous garder dans ses courants d'influence. La plasticité du code nous y rend perméable. Internet s'est refermé. L'utopie d'un contre-pouvoir médiatique, échappant à celui des États-entreprises centralistes est déçue. Nous devons dépasser ce triste constat souvent nostalgique.

Formons-nous les unes les autres à une meilleure hygiène et défense numérique, à notre échelle, à notre rythme ; prenons les devants. N'attendons pas d'être inculpées pour nous sentir concernées, l'anarchie, c'est prendre le maquis numérique, ouvrir des fanzines et revues, dire « non, je n'ai rien à déclarer », s'y habituer, se taire sans en avoir honte. Ne pas regarder ailleurs, croire quand le pire nous est confié, lire entre les lignes, mais aussi accepter, préserver et chérir le droit au silence et à l'oubli. Et, dans le même geste, demander – exiger – des comptes à ceux/elles que l'impunité protège. Rendre indéboulinables nos serveurs et réseaux de mémoire car nous n'oublions pas, nous ne pardonnons pas. Par les réseaux ingouvernables, faire circuler, amplifier les leaks, soutenir les bifurcations. L'anarchie, c'est reprendre du pouvoir sur nos habitabilités techniciennes. C'est l'œuvre d'une vie collectiviste.