Helen Nissenbaum & Finn Brunton

Obfuscation

A Report

C&F éditions

Dans la même collection :

Giorgio Griziotti, *Neurocapitalisme*
Pouvoirs numériques et multitudes.
Traduit de l'italien par Fausto Giudice.
ISBN 978-2-915825-82-4

Stéphane Bortzmeyer, *Cyberstructure*
L'Internet, un espace politique.
ISBN 978-2-915825-97-9

Chez le même éditeur :

Tristan Nitot, *Surveillance://*
Les libertés au défi du numérique : comprendre et agir.
ISBN 978-2-915825-65-7

danah boyd, *C'est compliqué*
Les vies numériques des adolescents.
Traduit de l'anglais par Hervé Le Crosnier.
ISBN 978-2-915825-58-9

Catalogue complet : https://cfeditions.com

Édition originale : *Obfuscation : a user's guide for privacy and protest*
Helen Nissenbaum and Finn Brunton, MIT press, 2015.

Traduit de l'anglais (États-Unis) par Elena Marconi, avec le soutien de Gauthier Verbeke et Emmanuel Vergès pour l'association OptinOptout.
La traduction a reçu le soutien du Centre national du Livre.

ISBN 978-2-915825-92-3 / Collection Société numérique, ISSN 2647-1493.

C&F éditions, avril 2018
35C rue des rosiers – 14000 Caen

Helen Nissenbaum & Finn Brunton

OBFUSCATION

La vie privée, mode d'emploi

Traduit de l'anglais (États-Unis) par Elena Marconi
avec la collaboration de
Gauthier Verbeke et Emmanuel Vergès
pour l'association OptinOptout

Préface par Laurent Chemla

C&F éditions
2019

Table des matières

Préface

Laurent Chemla

Soyons honnête : quand C&F éditions m'a proposé d'écrire une préface pour *Obfuscation*, ma première réaction (avant même l'habituel « Pourquoi moi ? ») fut de me demander qui avait bien pu faire un livre entier sur un thème aussi pointu.

Et puis je l'ai lu.

À moins d'être tombé par hasard sur ce texte, ce n'est pas une découverte pour vous, les pages des journaux en étant dorénavant pleines : notre vie privée n'est plus menacée ; elle est cacochyme, agonisante, voire déjà réduite à l'état de zombie, fiction constitutionnelle tout juste bonne à nous faire croire que l'on conserve encore quelques secrets à l'abri des GAFAM et du gouvernement.

Si les révélations d'Edward Snowden ont servi à quelque chose, c'est au moins à dessiller nos paupières sur l'étendue de la surveillance à laquelle nos vies sont soumises.

Face à cette réalité, deux réactions sont possibles.

La première, la plus facile, c'est de se retourner et de continuer à dormir. C'est la position dite du « si tu n'as rien à cacher, alors tu n'as rien à craindre ». Je l'avoue, j'ai longtemps adopté cette solution, jusqu'à ce qu'enfin un des arguments des défenseurs de la vie privée me convainque que j'avais tort. Avec le recul, j'ai intégré l'idée qu'*in fine* la

démocratie ne peut exister sans intime conviction, et donc sans intimité. Si vous faites partie des dormeurs, vous pourriez trouver dans ce livre – parmi d'autres – l'argument qui vous réveillera, vous aussi. Tant pis pour votre sommeil.

L'autre option, bien sûr, c'est d'essayer de se libérer de cette surveillance.

D'un point de vue pragmatique, c'est presque impossible. Dans une société numérisée, tous nos actes laissent des traces, partout, toujours. Nos objets connectés nous suivent jusque dans les toilettes, nos moyens de paiement espionnent tous nos achats, nos amis sont en ligne… la déconnexion totale est de plus en plus problématique. Les efforts nécessaires pour limiter un tant soit peu la dissémination de nos données personnelles deviennent démesurés, d'autant plus que l'on a rarement conscience de tout ce que nous laissons traîner derrière nous.

Dans ces circonstances, tout projet de libération apparaît de prime abord utopique. À peine peut-on espérer entrer en résistance. Et, puisque l'on utilise le vocabulaire de l'histoire avec ces deux termes franchement connotés, il peut être intéressant de comprendre comment nous en sommes arrivés là, pour mieux réfléchir aux moyens d'en sortir.

Si vous êtes assez vieux, vous vous souviendrez comme moi d'une époque où la seule idée d'être filmés dans le métro nous était insupportable ; où nous pouvions décider de ne pas rendre public notre numéro de téléphone en optant pour la « liste rouge » ; où l'idée d'une interconnexion des fichiers de l'administration causait un tel rejet qu'une loi « Informatique et Libertés » était votée ; où chacun luttait contre le « Programme Échelon » de filtrage des contenus par la NSA en ajoutant quelques mots-clés provocateurs en signature de tous ses messages (déjà, l'obfuscation était présente) ; et où Internet était – à l'inverse du modèle français du Minitel – basé sur la décentralisation (on parlait de « placer l'intelligence aux extrémités plutôt qu'au centre du réseau » : nous en sommes désormais très très loin).

Depuis, les pratiques ont changé. Vous vous filmez sans doute vous-même pour devenir youtubeur, vous préférez probablement utiliser les mêmes médias sociaux centralisés que vos amis, et vous trouvez certainement très simple de n'avoir à vous identifier en ligne qu'une

fois pour toutes, et n'hésitez pas à fournir votre zérosix pour recevoir les notifications de vos outils de surveillance numérique.

Que s'est-il passé ?

Je n'ai bien entendu pas les réponses, seulement quelques pistes, et toutes ne sont pas numériques, loin de là. Par exemple l'arrivée de la télé-réalité a sans doute contribué à réduire, dans notre *koinos kosmos*, la valeur sociale de la vie privée. L'évolution technique, qui nous permet de passer la soirée entre potes pendant que Bébé dort dans sa chambre, surveillé par sa babycam, n'a certainement pas aidé à renforcer notre résistance à la vidéosurveillance. La montée du terrorisme a permis de faire passer des lois toujours plus attentatoires aux libertés publiques, sans aucun coût politique… Le progrès social vers le « zéro risque » nous pousse naturellement à accepter la perte d'un certain degré de liberté, en échange d'un monde que nous espérons un peu plus sûr : radars routiers, traçabilité des aliments du producteur jusqu'au consommateur, limite de plus en plus basse des montants autorisés pour un paiement en liquide en sont encore d'autres exemples.

Clairement, la « valeur vie privée » chute en bourse. Ne nous étonnons pas si l'État n'y investit plus aucune ressource.

Au contraire même : dès qu'il en a l'occasion, le pouvoir n'hésite jamais à utiliser tout ce qui lui permet de mieux contrôler les populations. C'est dans son ADN. La perte de « valeur » de la vie privée dans les mentalités, associée à la baisse radicale du coût de la surveillance généralisée, la centralisation de nos données dans une poignée d'énormes silos simplifiant beaucoup le travail, rend l'équation économique et politique très rentable. Beaucoup plus rentable sur ces deux plans que la défense d'une démocratie respectueuse des libertés publiques, qui nécessiterait un discours complexe et qui ne rencontrerait que peu d'échos dans l'imaginaire collectif moderne.

Autrement dit, pour le pouvoir et les GAFAM, c'est tout bénef.

Pour ceux qui – comme moi – espèrent encore… c'est pas gagné, les copains.

Nous sommes en situation de faiblesse, face à des forces démesurées qui semblent occuper des places fortes quasi imprenables. Dans une telle position, j'imagine que Sun Tzu nous conseillerait d'éviter le

combat et de nous retirer du champ de bataille. Mais quand l'ennemi est partout, c'est assez difficile.

Quel espoir nous reste-t-il ?

Puisque nous sommes en résistance, alors il ne nous reste guère que l'option de la guérilla. C'est la force des faibles. Agir là où l'ennemi est le plus fragile, trouver les failles et nous y engouffrer, encore et encore, jusqu'à, peut-être, le faire reculer. C'est en tout cas l'option choisie par Helen Nissenbaum et Finn Brunton dans leur ouvrage.

Si l'équation est économique, l'idée de renchérir la surveillance semble devoir venir en tête de liste. En ce domaine, chacun peut agir. À son niveau d'abord en adoptant une hygiène numérique, certes inconfortable, mais dont les résultats sont rapidement tangibles : prendre le temps de mieux paramétrer nos outils pour limiter les droits que nous accordons sur l'utilisation de nos données personnelles n'est pas inutile ; choisir un autre fournisseur d'adresse email que Google permet de limiter l'énorme concentration actuelle ; réfléchir – un peu – avant de publier des informations sur nous-mêmes et sur nos proches, aux usages qui pourront en être faits, tant aujourd'hui que demain, pourquoi pas ?

Qui sait de quoi demain sera fait, et qui sera à la tête de l'État pour décider si nos photos, aujourd'hui innocentes, doivent nous conduire un jour dans un centre de rééducation ?

Bien sûr il est toujours tentant de conseiller la déconnexion, sinon du monde numérique (c'est illusoire : il est partout) au moins de tel ou tel monstre centralisateur. Mais souvent, c'est impossible. Nos amis sont sur Facebook, et y resteront même si nous le quittons. Nos contacts utilisent tous Gmail, et même si nous décidons d'utiliser un autre fournisseur nous continuerons de leur écrire, à eux et donc à Google. Pour autant, le fait de morceler nos données plutôt que de toutes les placer dans le même panier ne peut que rendre notre surveillance un peu plus complexe, et donc un peu plus chère. Inutile, sans doute, à l'échelle individuelle, mais potentiellement tangible – et donc facteur d'affaiblissement – à l'échelle du groupe humain.

Dans cette même optique, bien sûr, l'obfuscation prend tout son sens. Il suffit de constater ce que deviennent les « recommandations » d'Amazon lorsque, au lieu de nos achats habituels, nous utilisons

notre compte pour faire un cadeau (sans le décrire comme tel lors de la validation, évidemment) : l'algorithme est perdu, et avec lui une part de notre portrait numérique. N'importe quel avocat sait que l'on doit communiquer le maximum de pièces à son adversaire, de préférence à la veille d'une audience ; ce n'est pas pour rien. Ce n'est pas non plus uniquement pour garantir une organisation horizontale que tous les participants de la ZAD de Notre-dame des Landes se prénomment Camille ; c'est aussi pour ralentir – un peu – l'identification des présents. Ce n'est pas non plus pour faire joli que l'on a inventé la stéganographie : le fait de cacher un message dans une masse de données rend presque impossible son identification en tant que message.

Ce ne sont que quelques exemples, parmi tous ceux présentés dans ce livre, de l'enjeu de l'obfuscation. Ce ne sont que quelques aiguilles plantées dans la figurine de la surveillance généralisée, mais qui dégagent des espaces un peu plus vivables, où la surveillance serait un peu moins envahissante, et surtout un petit peu plus chère. À force, à force, tel ou tel État désargenté finira peut-être par choisir un modèle sécuritaire un peu moins massif : on a (encore un peu) le droit de rêver.

Et puisqu'on parle d'économie, de ZAD et de rêve…

Une autre des raisons qui nous ont conduit dans la situation présente, découle sans doute à de la façon dont s'est construit le modèle dominant de l'économie actuelle d'Internet. Parti de l'utopie des pionniers, qui voyaient le libre partage des ressources et des connaissances comme un levier pour créer une société plus juste (pour résumer beaucoup), Internet s'est démocratisé avec l'idée que tout y était, sinon gratuit, au moins d'accès libre.

Et (toujours en simplifiant beaucoup) lorsque les marchands s'en sont emparés, ils ont dû faire avec cette idée. Ceux qui choisissaient un modèle fermé, souvent payant, ont disparu (qui se souvient de Compuserve ou d'AOL ?), tandis que ceux qui proposaient un accès libre (d'aspect gratuit) sont restés. Bien sûr l'impératif de profit qui préside à la société marchande étant toujours là, ce sont nos données qui paient ce modèle, et la publicité qui finance le tout. Et bien sûr, plus vous accumulez de données mieux vous pouvez vendre d'espace

publicitaire, et plus vous disposez de moyens pour accroître encore vos sources de données.

C'est ainsi qu'on se retrouve *in fine* avec un tout petit nombre d'énormes mastodontes qui centralisent la quasi-totalité des informations privées qui constitue une grande part de nos vies.

Et ce fut d'autant plus aisé que, pendant ces années décisives, nous (hackers, activistes, défenseurs des libertés et autres rêveurs) sommes restés très largement passifs. « Google ? Oh ça va, c'est des hackers tout comme nous qui l'ont créé, ça peut pas partir en vrille ». «Facebook ? Un truc de débutant, ça marchera jamais. Occupons-nous plutôt d'inventer des trucs moches et sans documentation, mais libres, pour être certains que seuls nos semblables les adoptent ». Je caricature à peine.

Le réveil n'a pas été facile-facile.

Attaquer ce versant-là du capitalisme de surveillance ne va pas non plus l'être (facile-facile). On risque d'avoir besoin de très gros mousquetons, ou alors de beaucoup, beaucoup de temps. Et on en a peu. Sans parler des premiers de cordée, qui nous manquent aussi. Quelle entreprise à peu près respectueuse de la vie privée, aujourd'hui, est de taille à lutter à armes un tant soit peu égales avec Apple, Amazon, Microsoft, Google ou Facebook ?

Plus sérieusement, il me semble illusoire d'espérer que le secteur marchand puisse s'emparer d'un tel combat sans tomber rapidement du côté obscur (ou se faire racheter à bon compte par ce dernier). Et difficile d'imaginer les États s'en charger, eux qui dans ce cadre sont les alliés objectifs de « l'ennemi ». Pour autant, la lutte politique n'est ici pas tout à fait sans espoir. Car si le pouvoir est du côté des GAFAM quand il s'agit de surveiller la population, il y est très opposé dès qu'il est question d'argent. Des progrès comme la Directive européenne du RGPD (Règlement général de protection des données) prouvent que si l'on aiguillonne la poupée de l'État autour des questions économiques, elle peut revenir se placer du côté des libertés numériques. Bien sûr une telle marionnette n'agit que pour échanger un peu de pouvoir contre beaucoup d'argent (l'argent des contraventions contre le pouvoir de surveillance), mais tout ce qui peut affaiblir le modèle économique

hégémonique de « la gratuité contre vos données » est bon à prendre, au point où nous en sommes.

À condition, bien sûr, que « nous » soyons en mesure de proposer un autre modèle.

Quelques pistes existent. Pas les plus rectilignes, c'est entendu, mais cependant…

D'abord on pourrait tout simplement abandonner le numérique : ceux qui prédisent l'effondrement du capitalisme pensent avant tout à la rupture de l'infrastructure énergétique qui sous-tend toute industrie.

Pas de courant, pas d'Internet marchand.

Bon, OK, pas d'Internet du tout. Ni de civilisation sans doute, OK. Mais c'est une piste crédible, voire probable.

Ou sinon…

Reprenons nos problématiques: la vie privée n'a presque plus aucune valeur aux yeux de nos contemporains ; le grand public semble (c'est surprenant) privilégier les services gratuits aux services payants, ce qui conduit inévitablement à la centralisation des données et donc à un coût très faible pour les États et les GAFAM dans leur besoin de surveillance de masse.

On entend souvent ceux qui disent que, dans l'histoire, la vie privée est un phénomène récent, qui n'existait pas à l'échelle du village et qui est « donc » appelé à disparaître à l'échelle du « village global ». On entend moins souvent l'idée qu'à l'époque où la civilisation était à l'échelle du village, le capitalisme n'était pas encore le modèle économique dominant. Or, et ce n'est peut-être pas tout à fait décorrélé. On voit, depuis l'avènement de la civilisation numérique, revenir un usage depuis longtemps oublié : celui des communs.

Un commun est une ressource, naturelle ou culturelle, accessible à tous les membres d'un groupe humain. Cette ressource est partagée entre tous et entretenue au bénéfice de tous selon une gouvernance définie en commun. C'est, par exemple, le cas d'une grande majorité des logiciels libres. C'est aussi le cas d'un service comme Wikipédia, mais aussi du mouvement Nuit Debout, ou de la ZAD de Notre-Dame des Landes. C'était d'ailleurs le modèle (largement corrompu depuis) de l'Internet des origines, et celui qui, dans notre passé villageois,

présidait à l'usage des forêts et des pâturages : même si ceux-ci appartenaient au domaine de tel ou tel seigneur local, nos ancêtres avaient le droit d'y faire paître leurs bêtes ou d'aller y chercher du bois mort pour leur feu.

Le capitalisme n'est venu, plus tard, qu'avec les clôtures, les villes, et la marchandisation des ressources communes.

Peut-on imaginer revenir, ne serait-ce qu'un peu, à un modèle d'Internet basé sur les communs numériques ? Ce n'est pas totalement irréaliste : après tout, il n'est pas si éloigné le temps où le plus gros hébergeur français, celui qui faisait vivre la majorité des premiers sites web, était entièrement gratuit, libre, et sans publicité. Altern.org ne vivait que par l'argent que gagnait son inventeur en fournissant d'autres services. Bien sûr il aurait pu gagner davantage en vendant son service, mais il n'en avait pas besoin. Je sais, c'est dingue.

Mais pas totalement dingue. La preuve ? Wikipedia, encore. Open Street Map, idem. Entre autres.

Imaginons. Imaginons de multiples communs numériques. Quantité de services se créant, basés non sur la publicité mais sur le bénévolat, le mécénat, ou, sacrilège, sur le paiement d'usagers satisfaits !

Si nous sommes capables (et certains s'y emploient) de montrer au public, à tout instant, la façon dont sa vie est surveillée, au lieu de le lui cacher derrière des montagnes de cookies, de CGU à rallonge et de consentement en un clic, peut-être alors se rendra-t-il mieux compte de la valeur de sa vie privée, et du prix que lui coûtent vraiment les services « gratuits » des GAFAM. Et s'il entrevoit, même un tout petit peu, que ce prix est celui de sa liberté, alors peut-être (et cet espoir est déjà énorme tant les forces en présence sont inégales) acceptera-t-il plus facilement d'utiliser quelques services payants supplémentaires qui protègent sa vie privée, et plus largement la démocratie dont elle est une pierre fondatrice.

En multipliant le nombre des services en ligne que nous adoptons, et pour peu que ceux-ci soient basés sur autre chose que le capitalisme de surveillance, alors nous renchérirons d'autant le prix de cette surveillance. Si dans le même temps nous sommes capables d'augmenter, dans l'esprit du public, la valeur de la vie privée, alors nous fragiliserons

d'autant le modèle économique actuel du web et des médias sociaux. Et la société de surveillance.

Finalement, tout se résume, encore, à l'économie. C'est presque désespérant.

Alors, en attendant, on peut au moins commencer sur ce chemin en ayant recours à l'obfuscation.

Helen Nissembaum

Helen Nissembaum est professeure de Sciences de l'Information et de la Communication à l'Université Cornell Tech, après avoir exercé à l'Université de New York (NYU) où elle dirigeait l'Information Law Institute. Elle est docteur en philosophie de l'Université Stanford et a reçu en 2014 le Barwise Prize de l'American Philosophical Association qui récompense les travaux au confluent de la philosophie et de l'informatique.

Finn Brunton

Finn Brunton est maître de conférences à l'Université de New York (NYU) dans le département Média, Information et Communication. Ses travaux se concentrent sur l'adoption, la modification et l'usage détourné des médias numériques, sur la cryptographie et les diverses cultures du réseau. Il a obtenu en 2013 le prix PROSE remis par l'association des éditeurs américains pour ses livres sur l'informatique et la société.

Introduction

L'objectif de ce livre est de provoquer une révolution. Sûrement pas une révolution de grande ampleur. Enfin pas au début. Notre révolution ne se basera pas sur des réformes radicales, elle n'amènera pas un « An 01 » d'une société totalement réinventée. Elle n'impliquera pas l'adoption passive et homogène d'une nouvelle forme de technologie. Notre révolution s'appuie sur des éléments préexistants (ce qu'un philosophe appellerait des outils « à portée de main », ou un ingénieur des composants informatiques de base), facilement identifiables au quotidien et présents dans des films, des logiciels, des romans policiers et même dans le monde animal. Même si des dictateurs, des régimes autoritaires et des polices secrètes peuvent (et ils l'ont déjà fait) s'approprier sa terminologie et sa méthode, notre révolution s'adresse d'abord à ceux qui œuvrent au niveau local, aux usagers lambda et à la marge du système, à ceux qui ne sont pas en position de dire non, d'exercer un droit de retrait ou d'avoir le contrôle sur leurs données personnelles. Nous concentrons nos efforts pour affaiblir l'actuelle surveillance numérique et l'emporter sur son système. Pour la contourner, pour ne pas la subir, pour la refuser tout simplement, pour la saboter délibérément, ou pour imposer des conditions générales de service selon les règles voulues par l'*usager*, la boîte à outils existe déjà – ou est en voie de constitution.

Nous y apporterons notre contribution théorique et technique. En fonction de l'adversaire, en fonction des objectifs poursuivis et des

ressources disponibles, nous fournirons les méthodes pour gagner du temps, pour dissimuler nos données au regard de ceux qui les tracent, ou pour brouiller les résultats de leurs analyses ; ou alors nous révélerons les stratégies pour désobéir de façon provocatrice, pour soutenir toute protestation collective et toute revendication individuelle, quelle que soit sa portée. Nous tracerons le schéma général par des exemples avérés ou émergents, afin de repérer les orientations à suivre et définir des ensembles homogènes de moyens, de stratégies et d'actions concrètes à mener sur le terrain. Ce corpus détermine l'espace où aura lieu notre petite grande révolution. Et le drapeau sous lequel convergeront nos efforts s'appelle *Obfuscation*.

En quelques mots, *l'obfuscation consiste à produire délibérément des informations ambiguës, désordonnées et fallacieuses et à les ajouter aux données existantes afin de perturber la surveillance et la collecte des données personnelles*. Une chose simple mais qui ouvre sur des applications et des usages nombreux et complexes. Pour un développeur ou un designer, intégrer l'obfuscation dans ses programmes lui permettra de garantir la sécurité des données des futurs utilisateurs – y compris les leurs ou celles d'un éventuel acheteur – tout en fournissant des services qui nécessitent la collecte et l'utilisation d'informations personnelles, comme les réseaux sociaux, la géolocalisation, ou autre. Avec l'obfuscation, les services publics et les agences gouvernementales pourront réaliser leurs besoins de collecte de données tout en réduisant le risque d'abus. Pour l'individu ou le groupe qui souhaite vivre dans le monde moderne sans devenir l'objet d'une surveillance numérique omniprésente (et qui dit surveillance, dit enquêtes et poursuites), l'obfuscation sera l'arme pour se défendre, gagner du temps ou dissimuler ses traces numériques derrière une cacophonie des signaux : une ressource modeste, certes, tel le grain de sable qui bloque l'engrenage !

De cette révolution, ce livre est le point de départ.

Notre projet nous a amenés à repérer des similitudes intéressantes provenant de champs disparates au sein desquels ceux qui sont obligés d'être visibles, intelligibles et audibles ont réagi en enfouissant les signaux pertinents sous des strates nébuleuses de signaux trompeurs. Fascinés par la diversité des situations dans lesquelles les gens

appliquent des méthodes d'obfuscation, nous avons présenté dans les chapitres I et II, une douzaine d'exemples différents mais qui ont un élément en commun : le contexte d'une menace de surveillance généralisée. Ces deux chapitres, qui composent la première partie du livre, constituent un répertoire des différentes formes que peut prendre l'obfuscation. Ils font ressortir le type de stratégie à adopter selon le but poursuivi et selon l'adversaire. Que ce soit sur un réseau social, devant une table de poker, ou dans le ciel de la Seconde Guerre mondiale ; que l'adversaire soit un système de reconnaissance faciale, le gouvernement de l'Apartheid en Afrique du Sud des années quatre-vingt, ou la personne assise de l'autre côté de la table, le recours à la tactique appropriée d'obfuscation contribue à la protection de la vie privée et renverse le rapport de force dans la relation de collecte, d'observation et d'analyse de données. À travers les exemples exposés dans ces deux chapitres, nous présentons une panoplie de situations et d'usages qui seront source d'inspiration pour tout un chacun et apportons des éléments de réponse à la question : qu'est-ce que l'obfuscation peut offrir à chacun d'entre nous ?

Dans le chapitre I, les cas analysés sont organisés comme un récit afin d'éclairer les questions fondamentales que l'obfuscation soulève, et de décrire les méthodes principales qui seront explorées et débattues dans la seconde partie du livre. Le chapitre II traite rapidement quelques cas particuliers, et illustre l'éventail et la variété des applications de l'obfuscation tout en expliquant les concepts qui sont sous-jacents.

Les trois chapitres suivants analysent des questions fondamentales et permettent d'acquérir une connaissance plus fouillée de l'obfuscation. Nous nous interrogerons alors sur le « pourquoi » et verrons quel rôle elle peut jouer dans les différents systèmes de confidentialité et de protection de données personnelles ; nous aborderons les problèmes éthiques, sociaux et politiques que pose l'emploi de l'obfuscation ; nous analyserons les différentes stratégies et évaluerons si, et dans quel contexte particulier, l'obfuscation fonctionne ou pourrait fonctionner. Ce cheminement nécessite d'appréhender les points forts et les points faibles de cette méthode et de voir en quoi elle se différencie des autres.

C'est pour cette raison que nous avons titré les chapitres de III à V par des questions.

Le chapitre III pose la première : « Pourquoi l'obfuscation est nécessaire ? ». En y répondant, nous expliquons comment relever les défis actuels liés à la vie privée en contexte numérique grâce à l'obfuscation. Nous montrons comment l'obfuscation peut être utilisée pour contrer l'asymétrie informationnelle, c'est-à-dire lorsque la collecte de données personnelles et leur exploitation sont faites dans des circonstances incompréhensibles, avec des finalités opaques et selon des modalités mystérieuses. Elles seront partagées, achetées, vendues, réglementées, analysées : avec quelles conséquences sur la vie des gens ? Est-ce que je vais avoir l'emprunt que j'ai sollicité ? ou l'appartement pour lequel j'ai déposé un dossier ? Quelle est la valeur d'un homme pour un assureur ? Et pour un banquier ? Quels prospectus publicitaires inonderont ma boîte aux lettres ? Comment se fait-il qu'autant de firmes et de fournisseurs de services savent que cette jeune fille est enceinte, ou que le voisin essaie de se désintoxiquer, et qu'il envisage de changer de métier ? Pourquoi allouer les ressources selon les catégories socio-économiques, les groupes ethniques ou l'origine géographique, voire même le quartier ? Allons-nous tous nous retrouver « sur une liste de personnes à risque », comme c'est le cas actuellement dans le cadre de l'inquiétante lutte antiterroriste ? Toutes ces situations anodines et à l'apparence banale, finissent par avoir des répercussions importantes. Et c'est là que l'obfuscation joue tout son rôle : non pas pour supplanter le système de gouvernance, l'écosystème entrepreneurial ou l'environnement technologique en place ; ni comme solution passe-partout (nous l'avons dit, il s'agit d'une révolution délibérément limitée et décentralisée), mais plutôt pour concourir à la défense de la vie privée. Plus particulièrement l'obfuscation est une stratégie qui s'adapte à tous ceux qui n'ont jamais accès à d'autres voies de recours, que ce soit à un moment donné de leur vie ou plus généralement ; à tous ceux qui, et cela arrive, ne sont pas en capacité de faire correctement appel aux outils de protection de la vie privée, parce qu'ils se trouvent dans une position d'infériorité dans la relation pouvoir-information.

Cependant chaque technique d'obfuscation soulève aussi des questions d'ordre éthique et politique. Avant d'y recourir, il faut s'interroger sur l'impact qu'elle pourrait avoir et les problèmes qu'elle pourrait engendrer, que ce soit dans les politiques sociales ou dans les médias sociaux. « L'obfuscation est-elle légitime ? », c'est la question que nous nous posons au chapitre IV. Ne sommes-nous pas en train d'inciter les gens à mentir ? À être sciemment inexacts et à « polluer » par un bruit potentiellement dangereux, les bases de données pouvant avoir des applications commerciales et civiques ? Ceux qui utilisent gratuitement les services des plateformes commerciales, ne le font-ils pas aux crochets des utilisateurs honnêtes ? De ceux qui paient pour des services (et la publicité ciblée qui va avec) en rendant leurs données d'utilisation disponibles ? Si ces pratiques se généralisent, n'allons-nous pas gaspiller collectivement la puissance de calcul et la bande passante ? Dans le chapitre IV, nous relevons ces défis et décrivons le raisonnement moral et politique, qui permet de juger, dans quel cas précis l'obfuscation est acceptable ou inacceptable.

Le dernier chapitre décrit ce que l'obfuscation peut ou ne peut pas réaliser. Comparée à la cryptographie, elle peut être considérée comme une pratique contingente et précaire. Le chiffrement permet en effet de déterminer avec précision le niveau de sécurité à appliquer pour résister aux tentatives de déchiffrement par la force brute, en ajustant les paramètres comme la longueur des clés, la puissance de traitement et le temps nécessaire à décoder. Avec l'obfuscation une telle précision est rarement possible. En tant qu'outil pratique, sa force dépend en effet de circonstances réelles, de ce que ses utilisateurs veulent réaliser et de limites spécifiques auxquels ils peuvent être confrontés. Néanmoins complexité ne signifie pas chaos et la clé de la réussite repose sur l'attention accordée aux relations internes aux systèmes. Au chapitre V, nous identifions six objectifs communs pour les projets d'obfuscation et nous les mettons en corrélation avec le design correspondant. Les objectifs principaux incluent le fait de gagner du temps, de se camoufler, de se cacher, d'éviter le contrôle, de brouiller le profilage et de participer à des mouvements de protestation. Pour le design, nous analysons le projet d'obfuscation en prenant en considération différents éléments

constitutifs, et notamment s'il est collectif ou individuel, connu ou inconnu, sélectif ou général, à court ou à long terme. Par exemple, en fonction de l'objectif, l'obfuscation pourra être un échec si l'adversaire connaît les techniques employées ou au contraire il vaudrait mieux qu'il sache que les données ont été polluées, comme c'est le cas dans une protestation collective, les techniques contre le ciblage personnalisé et le démenti. Tout cela dépend évidemment des ressources à disposition de l'adversaire, c'est-à-dire, le temps, l'énergie, l'attention, et l'argent qu'il est prêt à dépenser pour identifier et éliminer la source de camouflage. Ce raisonnement est prometteur parce qu'en partant d'une analyse de cas, nous apprenons comment adapter au mieux l'obfuscation à sa finalité. En conclusion, l'obfuscation peut-elle fonctionner ? Oui, mais seulement dans un contexte déterminé.

Et maintenant, allons-y !

Helen Nissenbaum & Finn Brunton

OBFUSCATION

La vie privée, mode d'emploi

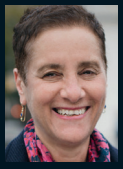
Traduit de l'anglais (États-Unis) par Elena Marconi
avec la collaboration de Gauthier Verbeke et Emmanuel Vergès
Préface par Laurent Chemla

> **« Où le Sage cache-t-il une feuille ? Dans la forêt.**
> **Mais s'il n'y a pas de forêt, que fait-t-il ?…**
> **Il fait pousser une forêt pour la cacher. »**

L'obfuscation, magistralement illustrée par l'auteur de roman G. K. Chesterton.

Dans ce monde de la sélection par des algorithmes, de la publicité ciblée et du marché des données personnelles, rester maîtres de nos actions, de nos relations, de nos goûts, de nos navigations et de nos requêtes implique d'aller au delà de la longue tradition de l'art du camouflage. Si on peut difficilement échapper à la surveillance numérique, ou effacer ses données, il est toujours possible de noyer nos traces parmi de multiples semblables, de créer nous-mêmes un brouillard d'interactions factices.

Quels en sont alors les enjeux et les conséquences ? Helen Nissenbaum et Finn Brunton ayant constaté l'asymétrie de pouvoir et d'information entre usagers et plateformes dressent le bilan, proposent des actions et prennent le temps de la réflexion : pourquoi et comment reconquérir son autonomie personnelle ? Comment résister éthiquement avec les armes du faible ? Comment réfléchir ensemble à ce que l'obfuscation nous fait découvrir sur l'influence mentale exercée par les puissants du numérique ?



Helen Nissembaum est professeure de sciences de l'information et de la communication à l'université Cornell Tech. Elle est docteure en philosophie de l'université Stanford et a reçu en 2014 le Barwise Prize de l'American Philosophical Association.
Finn Brunton est maître de conférences à l'université de New York (NYU) dans le département médias, information et communication. Il a obtenu en 2013 le prix PROSE remis par l'association des éditeurs américains pour ses livres sur l'informatique et la société.

20 €
ISBN 978-2-915825-92-3
ISSN 2647-1493
http://cfeditions.com
imprimé en France

Avec le soutien du CNL Centre national du livre

9 782915 825923