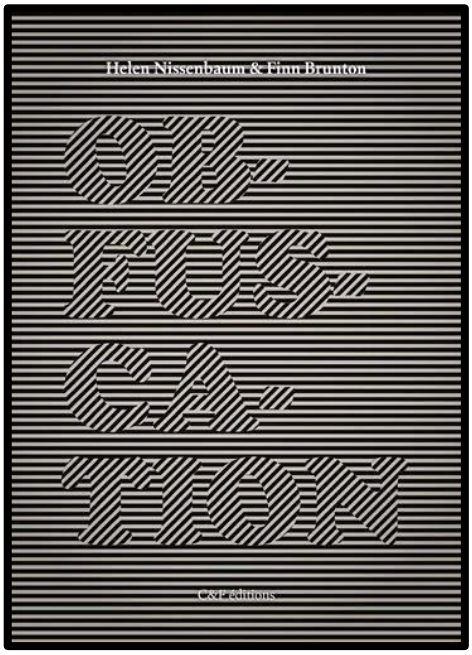
# OBFUSCATION
# LA VIE PRIVEE, MODE D'EMPLOI

Nissenbaum, Brunton, Chemla, Marconi, 2019. C&F Editions.

*Nolwenn Voiturier, Lara Dourthe, Laurine Sauvage, Renan-Anglade Charles-Cius*




Le livre que nous allons vous présenter est intitulé : "Obfuscation. *La vie privée : mode d'emploi.*". Il a été écrit par Helen Nissenbaum, professeure de Sciences de l'Information et de la Communication à l'Université Cornell Tech., et Finn Burton, Maître de Conférences à l'université de New York dans le département médias, information et communication. Il s'intéresse à l'informatique dans la société.

Une définition que nous donne les auteur-e-s de l'obfuscation est que « l'obfuscation consiste à produire délibérément des informations ambigües, désordonnées et fallacieuses et à les ajouter aux données existantes afin de perturber la surveillance et la collecte des données personnelles ». Pour simplifier, il s'agit de noyer le poisson, de donner beaucoup d'informations à traiter, voire trop d'informations à traiter pour rendre toute personne incapable de démêler le vrai du faux.

Pour remettre en contexte la réception de l'ouvrage, il a été publié en 2015 au États-Unis à la même période que l'apparition du lanceur d'alerte Snowden. Aussi, aux États-Unis, ce livre a eu un écho important car Snowden a suscité une certaine prise de conscience de la part d'une partie des Américains du nord concernant la collecte de données privées.

Dans une première partie, nous vous parlerons du concept de *privacy*, dans une deuxième partie, nous traiterons les différentes asymétries qui structurent les relations entre les plateformes numériques et leurs usagers. Et enfin, dans une troisième partie, nous vous présenterons une partie critique concernant les points de vue des auteur·e·s et les nôtres.

## QU'EST-CE QUE L'OBFUSCATION ?

### *DEFINITION, CONTEXTE ET EXEMPLES*

Helen Nissenbaum définit l'obfuscation lors d'une conférence donnée au sein du MIT comme « la production, l'inclusion, l'ajout ou la communication de données trompeuses ambiguës ou fausses dans le but de se soustraire, de susciter la confusion ou de diminuer la fiabilité (et la valeur) des agrégateurs de données. » Autrement dit, l'obfuscation représente une technique d'obscurcissement car elle vise à masquer les données importantes dans une masse d'informations.

Le concept d'obfuscation s'inspire du camouflage animal en reprenant l'exemple de l'araignée aranéomorphe qui tisse des toiles afin de chasser et piéger ses proies. Durant cette action, l'araignée devient alors elle aussi vulnérable aux yeux de la guêpe, son principal prédateur. Pour éviter de se faire attraper, l'araignée va fabriquer des leurres qui lui ressemblent en tout point (même taille, même couleur, même reflet chatoyant). La technique de l'araignée est alors de placer des sosies un peu partout sur la toile. Elle se dissimule au milieu de « faux elles » ce qui lui permet ainsi d'être moins vulnérable aux yeux des guêpes et d'avoir le temps de fuir en cas de danger.

Durant la Seconde Guerre Mondiale, la stratégie de l'obfuscation a été utilisée par les résistants pour déjouer des radars militaires allemands. L'objectif des allemands était de tracer les avions des résistants afin de connaître leur position et de les pister. Le livre reprend l'exemple de radars militaires dans le ciel de Hambourg qui traçaient des avions en suivant la position de leurs points lumineux. La position était réactulisée à chaque nouvelle position d'antenne. L'obfuscation a permis d'inonder l'écran de traçage d'une multitude de points lumineux (faux signaux) afin de brouiller la trajectoire des vrais avions. Pour ce faire, un avion déversait dans le ciel une multitude de paillettes dorées qui étaient de petites feuilles noires recouvertes de papier argenté de la taille d'une demi-longueur d'onde de radar. En répondant exactement aux critères de captation des données des antennes, elles permettaient ainsi de brouiller les pistes.

Aujourd'hui, l'obfuscation peut être utilisée au quotidien pour lutter contre l'usage de nos données personnelles à des fins commerciales. Le logiciel "Track Me Not" a été lancé en 2006 par Daniel Howe, Helen Nissenbaum et Vincent Toubiana après l'affaire des logs d'AOL Search. AOL avait volontairement mis en ligne un document contenant les recherches effectuées par ses internautes américains. Près de 658 000 utilisateurs et les

millions de données issues de leurs recherches ont été diffusées sans le consentement de ces utilisateurs. L'objectif du logiciel TrackMeNot était alors de protéger les requêtes sur les moteurs de recherche en créant de faux signaux afin de dissimuler les vrais. Cette technique se place comme une stratégie de résistance à la surveillance de nos données. C'est un exemple concret de moyen pouvant être utilisé afin de lutter contre l'usage abusif de nos données personnelles.

### *PRIVACY : CAMOUFLAGE ET RISQUE*

Le concept de *privacy* est difficile à définir. Il peut être traduit par 'vie privée" mais recoupe également d'autres définitions en fonction de son contexte. D'après les auteur·e·s, la *privacy* désigne quatre concepts différents : "Au premier l'intégrité de la vie de famille, au deuxième le système de pouvoir étatique (contemporain ou futur), au troisième l'exploitation des données personnelles et leur valeur marchande, et au dernier l'anonymat, seul garant de l'épanouissement personnel". Ils sont partisans de l'adage "pour vivre heureux, vivons cachés". Les auteur·e·s développent alors des méthodes d'obfuscation en fonction de leurs objectifs et de ces différents concepts de *privacy*. Aussi, ils pensent que "la *privacy* est un concept à facettes qui nécessite de mobiliser une vaste gamme d'outils, de structure, de mécanisme, de règle et de pratique afin de le rendre concret et de le protéger".

Cependant, l'influence des GAFAM aujourd'hui est telle qu'il est impossible de se mettre en retrait en refusant de leur donner des informations. Le retrait n'est donc pas une solution pour les auteur·e·s car elle n'est pas viable. En effet, nous ne pouvons plus nous passer des services mis à disposition par les GAFAM : avoir une boite Gmail ou utiliser un GPS par exemple. Leurs services sont requis dans les domaines personnel, professionnel et social. Cette situation nous place, nous citoyens, comme impuissants. D'une certaine manière, ce fonctionnement nous est imposé. L'obfuscation est donc une réaction de légitime défense. Concrètement, pour les citoyens, le risque est réel. Il a été vu qu'aux États-Unis, certaines familles s'étaient vues refuser des crédits car les assurances, les banques et les agences de crédit avaient récupéré les données financières de ces familles, potentielles clientes. Les assurances et les banques les avaient alors jugées inaptes à rembourser un crédit. Aussi, si leurs données n'avaient pas été collectées à leur insu, ces familles auraient peut-être eu davantage de chance d'avoir un crédit. Pour éviter cette situation, l'obfuscation semble être la seule solution.

## JUSTIFICATION DE L'OBFUSCATION

Pour répondre à un certain nombre d'accusations, les auteur·e·s ont cherché à légitimer leur stratégie d'obfuscation. Ils ont décrit de nombreuses asymétries qui caractérisent les relations entre les GAFAM et les internautes.

### *ASYMETRIE INFORMATIONNELLE*

D'après les auteur·e·s, il existe une asymétrie informationnelle, entre les GAFAM d'une part et les usagers des plateformes d'autres part. Les usagers n'ont pas accès aux mêmes informations que les GAFAM qui récoltent leurs données personnelles et les utilisent à des fins lucratives et commerciales.

Les auteur·e·s structurent leur démonstration en trois parties/L'asymétrie informationnelle entre les GAFAM et leurs usagers opère à trois niveaux :

Premièrement, "*il faudrait savoir ce que l'on sait*". Par exemple, un usager faisant ses courses dans un supermarché sait qu'il est filmé parce qu'il voit une caméra de surveillance et qu'il a conscience de son savoir. La deuxième étape est de "*savoir ce que l'on ne sait pas*". Par exemple, l'usager a été filmé mais ne sait pas comment l'enregistrement sera utilisé ou s'il sera diffusé. Il a conscience de ne pas savoir. Enfin, la troisième et dernière étape est de "*ne pas savoir ce que l'on ne sait pas*". On pousse le questionnement en se demandant comment sera exploitée la vidéo, par qui, et surtout pourquoi. Ces questionnements sont infinis. L'usager peut à peine les formuler. Il ne peut pas savoir tout ce qu'il ne sait pas. L'asymétrie informationnelle est donc la principale asymétrie car concrète et observable au quotidien. Elle est aussi symbolique car le fait d'être filmé influence malgré eux les citoyens qui se savent observés en permanence. Cela peut créer un climat de méfiance et le sentiment d'un contrôle injustifié.

### *ASYMETRIE FINANCIERE, DE POUVOIR, RELATIONNELLE*

Les asymétries entre les GAFAM et les usagers lambda sont nombreuses. En plus de l'asymétrie informationnelle, on constate une asymétrie de pouvoir, une asymétrie financière et une asymétrie relationnelle.

Quand un utilisateur accède à une page internet, il se voit contraint d'accepter des "cookies". Il n'a, à ce moment, aucune autre alternative s'il veut bénéficier de ce service. Le fait que l'usager soit dans l'impossibilité de choisir d'être surveillé ou non, dans l'impossibilité de savoir ce qui sera fait de ses données et dans l'impossibilité de connaître les mesures prises, est rendu possible par un pouvoir asymétrique. Le pouvoir est indispensable pour collecter des informations, et les GAFAM ont actuellement plus de pouvoir que les usagers qui sont aujourd'hui dépendants de ses services.

A chaque fois qu'un usager fait les courses par exemple, il produit des données qui sont collectées grâce à sa carte de fidélité sans qu'il puisse y remédier. Les pouvoirs sont asymétriques car il est difficile pour l'usager de faire un choix concernant la collecte de ses données. Il y a un lien étroit entre l'obfuscation et l'asymétrie de pouvoir puisque les auteur·e·s définissent l'obfuscation comme une "méthode qui s'adapte aux situations dans lesquelles esquiver la surveillance n'est pas possible."

L'asymétrie financière se caractérise par l'exploitation de l'usage des données à l'insu des utilisateurs. Les GAFAM utilisent aujourd'hui ces données personnelles dans un but lucratif sans le consentement des usagers. Les GAFAM donnent une valeur marchande à la vie privée des usagers et les données collectées sont revendues à d'autres acteurs marchands. Le fait est que "les informations personnelles ont une valeur marchande" et ce n'est pas à celui qui a produit cette information qu'elle profite.

On note aussi une asymétrie relationnelle dans une relation de "pouvoir-savoir-risque" où la partie la plus faible, ici, les usagers, ne peuvent pas riposter de manière efficace contre la partie la plus forte, ici, les géants du web. L'asymétrie relationnelle vient du fait que les GAFAM connaissent bien mieux les usagers qu'eux ne connaissent les GAFAM. La collecte de données donne un pouvoir aux GAFAM qui peuvent alors influencer la vie quotidienne des usagers, que ce soit par la proposition de nouveaux services ou via les publicités personnalisées. Ils réalisent un ciblage publicitaire en fonction des données collectées en amont. Par exemple, un usager qui fait du « shopping » en ligne se voit proposer des publicités en lien avec ses recherches sur d'autres sites internet.

Selon les auteur·e·s, c'est à cause de ces asymétries que l'obfuscation est la seule solution au maintien de la *privacy*. Elle devient donc "l'arme des faibles".

## CRITIQUE DE L'OBFUSCATION

### *POINT DE VUE DES AUTEUR·E·S :*

*"Nous souhaitons convaincre nos lecteurs que pour faire face aux problèmes touchant la vie privée, l'obfuscation est dans certains cas la solution la plus concrète et la plus efficace, alors que dans d'autres situations elle représente LA meilleure solution.".*

Cette citation synthétise l'ambition du livre. Les auteur·e·s font la démonstration de l'utilité, de la nécessité et de la légitimité de l'obfuscation. Ils savent néanmoins que des critiques sont opposables mais s'en justifient.

A ceux qui pensent que l'obfuscation est une technique malhonnête car elle détourne des ressources, vise à induire en erreur et équivaut alors à un mensonge questionnable sur le plan éthique ; les auteur·e·s répondent en disant : "Puisque se défendre est une finalité qui légitime en soi l'accomplissement d'actes malhonnêtes, il faudrait être plus précis et dire que c'est la finalité de l'action qui permet d'établir si la méthode d'obfuscation, comme mentir, est moralement acceptable ou pas.". La malhonnêteté serait excusée par le contexte dans lequel nous nous trouvons. Les multiples asymétries de pouvoir, relationnelle et financière ne nous laissent donc pas d'autres choix que de mentir pour nous protéger. Les auteur·e·s justifient le droit à la "*privacy*" comme légitime. C'est pour

eux un acte de légitime défense : "l'arme des faibles". Cela leur permet d'expliquer la mise en place de l'obfuscation et du logiciel *Track Me Not*. Ce logiciel permet aux utilisateurs de dissimuler leurs données personnelles parmi une masse de données. En somme, les usagers ont besoin des services des géants du web. Ils trouvent des stratagèmes pour les utiliser gratuitement tout en protégeant leurs données personnelles.

### *NOTRE POINT DE VUE :*

Nous avons lu avec attention cet ouvrage et avons constaté un apport cohérent et structuré sur un sujet encore peu médiatisé: la collecte des données personnelles et l'obfuscation. Helen Nissenbaum et Finn Burton nous présentent de multiples exemples de l'obfuscation et nous donnent leurs raisons de la légitimer au regard de la puissance reconnue des GAFAM.

Nous pensons avoir bien cerné les enjeux auxquels répond l'obfuscation. Néanmoins, nous regrettons que les auteur·e·s ne proposent pas d'autres alternatives au phénomène de contrôle des données personnelles par les GAFAM. Le fait qu'ils aient choisi de nous présenter l'obfuscation comme unique solution ne nous laisse pas le choix quant à ce que nous estimons nécessaire ou non. Les GAFAM sont puissants et nous ne pouvons pas uniquement nous mettre en retrait de la société pour éviter la collecte de nos données. Cependant, la solution de l'obfuscation telle qu'elle est présentée nous semble plutôt radicale. En Europe, comme en France nous avons moins conscience de l'utilisation de nos données personnelles qu'aux Etats-Unis puisqu'en France nos données sont en partie protégées par la CNIL (Commission Nationale de l'informatique et des libertés) et par le RGPD (Règlement Général sur la protection des données). Les utilisateurs qui transmettent inconsciemment leurs données personnelles aux GAFAM ne se sentent pas directement en danger. Ils ne ressentent pas les risques et l'influence que les GAFAM peuvent avoir au quotidien.

Néanmoins, ce livre reste très bien documenté par rapport à ce phénomène. Il est utile et permet à tout le monde de se renseigner sur l'utilisation des données personnelles des usagers par les GAFAM, parfois méconnue du grand public. Il est d'autant plus important de communiquer sur ce sujet que de nouvelles réglementations tendent à être appliquées à ces GAFAM même s'ils s'y refusent pour le moment.

Nous conclurons cette synthèse en encourageant les lecteurs et internautes à consulter cet ouvrage car il concerne un grand enjeu du 21ème siècle.

**#CulturesNum** est un programme réalisé par les étudiants du **Master Communication des Organisations de l'Université Bordeaux Montaigne** sous la direction d'**Aurélie Laborde**, en collaboration avec **UNITEC**. Depuis 2016, des ouvrages récents sur la société numérique sont synthétisés pour mieux appréhender les questions de fond pour notre société : big data, smart-cities, post humanisme, avenir du travail et de la consommation, etc...