

La « datapulation » ou la manipulation par les données

Description

Interview de [Claude Castelluccia](#) – Propos recueillis par [Françoise Laugée](#)

Vous êtes directeur de recherche à l’Inria, sur quels sujets travaille actuellement l’équipe appelée Privatics que vous dirigez ?

L’équipe Privatics¹ de l’Inria (Institut national de recherche en informatique et en automatique) est localisée à Grenoble et à Lyon. Elle a pour objectif d’étudier les nouvelles menaces qui pèsent sur la vie privée introduites par la société de l’information et de concevoir des solutions préservant la vie privée. Nous travaillons sur des sujets aussi divers que l’anonymisation des données, la protection de la vie privée dans l’internet des objets, l’analyse des systèmes de surveillance et de profilage ou la transparence des algorithmes et des systèmes.

Le projet suit une approche multidisciplinaire. Il se concentre sur des questions techniques et scientifiques, mais il prend également en considération les aspects économiques, juridiques et sociaux de la vie privée. Nous collaborons notamment avec la Cnil (Commission nationale de l’informatique et des libertés) dans le cadre de la convention Cnil-Inria.

Pour ainsi dire, nous « payons », avec des informations qui relèvent de notre vie privée, l’accès à des services web personnalisés. Quel est le niveau de performance des techniques de profilage aujourd’hui ? Pour quels usages ? Et avec quels effets ?

CES TECHNIQUES D’ANALYSE PERMETTENT D’IDENTIFIER NOS ÉTATS ÉMOTIONNELS OU NOS PROFILS PSYCHOLOGIQUES

Nos données personnelles sont collectées et analysées par diverses entreprises ou entités à des fins de personnalisation, catégorisation ou de surveillance. Ces techniques d’analyse sont très puissantes et permettent, parmi d’autres choses, d’identifier nos états émotionnels ou nos profils psychologiques. Il a été montré que l’analyse des données Facebook peut identifier précocement les utilisateurs qui ont des tendances suicidaires².

Ces données sont collectées sur internet, lorsque nous visitons des sites web ou des réseaux sociaux, mais aussi dans le monde physique, grâce à nos téléphones portables. C’est ce qu’on appelle le « profilage physique³ ». En effet, les applications que nous utilisons sur nos téléphones intelligents collectent de

nombreuses données comportementales, qui permettent de nous géolocaliser. Cette géolocalisation sert, en outre, à identifier nos points d'intérêt.

Ce profilage est essentiellement effectué par des entités tierces à des fins de ciblage publicitaire ou de personnalisation de services. Il est également utilisé pour catégoriser les comportements des utilisateurs. Ces informations sont très utiles, notamment pour les banques ou les assurances lorsqu'elles souhaitent proposer un service à un client. Il existe aussi un vrai marché des données, collectées par des *data brokers* qui revendent ces données ([voir La rem n°46-47, p.77](#)). Finalement, ce profilage est également utilisé à des fins sécuritaires, comme l'ont montré les révélations de Snowden sur la collecte de masse effectuée par la NSA⁴.

CETTE GÉOLOCALISATION SERT À IDENTIFIER NOS POINTS D'INTÉRÊT

Les dangers de ce profilage sont multiples. Il permet de « catégoriser » les internautes, ce qui peut conduire à des risques de discrimination. Une assurance pourra décider de ne pas assurer une personne si son profil correspond à un profil « à risque ». Les risques et les dangers de ce type de catégorisation peuvent être importants comme on peut le voir avec les systèmes de « police prédictive » ou de « score social » en Chine⁵.

Un autre danger de ce profilage, et plus particulièrement de l'utilisation de ce profilage pour faire du ciblage, est ce qu'on appelle communément la « bulle de filtres » (*filter bubble*). La « bulle de filtres » désigne l'état d'isolement intellectuel et culturel dans lequel un internaute se retrouve lorsque les informations qu'il reçoit sur internet sont uniquement ciblées en fonction de son profil.

Qu'est-ce que la « datapulation » (data et manipulation) et pourquoi dites-vous que « comme notre infrastructure énergétique, notre infrastructure cognitive est critique » ?

Comme nous l'avons souligné précédemment, nos données personnelles sont utilisées à des fins de surveillance et de ciblage. La « dataveillance » (surveillance par les données) est la pratique qui consiste à collecter des données et des métadonnées dans le but de surveiller des individus.

Ce que l'on sait moins, c'est que nos données personnelles sont de plus en plus utilisées pour nous influencer, voire nous manipuler. C'est ce que j'appellerais la « datapulation » (la manipulation par les données). En contrôlant les informations que nous recevons en ligne et en les adaptant à nos comportements, un service comme Facebook peut être utilisé pour influencer nos comportements de clients, nos opinions, nos émotions, voire, comme le suggère l'affaire récente « Cambridge Analytica », nos choix politiques ([voir La rem n°48, p.90](#)). Ces manipulations, très étudiées en marketing comportemental (*neuromarketing*), sont les conséquences même du modèle économique de l'internet et de ses services « gratuits ». Il devient urgent de développer des solutions pour s'en protéger et sécuriser notre « infrastructure cognitive », qui est probablement au moins aussi critique que notre infrastructure énergétique ou de télécommunication.

NOS DONNÉES PERSONNELLES SONT DE PLUS EN PLUS UTILISÉES POUR NOUS INFLUENCER, VOIRE NOUS MANIPULER

Les techniques de manipulation par les données sont nombreuses et variées. On peut cependant les classer en trois grandes catégories :

1. les techniques basées sur la « manipulation informationnelle » ;
2. celles basées sur la « manipulation psychologique ou cognitive » ;
3. celles dont le but est de rendre l'exécution d'une action difficile ou de tromper l'utilisateur, ce que l'on appelle en anglais les *dark patterns*.

1. La manipulation informationnelle

Les techniques de cette catégorie tentent de modifier notre système cognitif en polluant les informations ou connaissances que nous utilisons pour le construire. C'est typiquement le cas des fausses informations publiées sur le web ou les réseaux sociaux (les *fake news*), dont l'objectif est d'influencer nos opinions, et parfois nos votes.

IL DEVIENT URGENT DE SÉCURISER NOTRE «INFRASTRUCTURE COGNITIVE»

Dans un rapport récent intitulé « Information Disorder : Toward an interdisciplinary framework for research and policy making » ([voir La rem n°45, p.62](#)), le Conseil de l'Europe fait la distinction entre deux classes de publications d'informations « nuisibles » :

- La désinformation consiste à diffuser une information fausse dans le but de nuire (on parle alors de dis-information ou *fake news* en anglais), ou par ignorance ou erreur (on parle alors de mal-

information (*mis-information* en anglais). Un exemple de dis-information est l'information, qui a circulé pendant la campagne présidentielle, prétendant faussement que la campagne du candidat Macron était financée par l'Arabie saoudite.

- La mal-information est une information correcte, souvent confidentielle ou privée, mais publiée à grande échelle dans un but spécifique. C'est l'exemple des courriels privés, volés et publiés sur internet pendant la dernière campagne présidentielle aux États-Unis.

On peut également ajouter à cette catégorie de manipulations les techniques de filtrage ou de censure de l'information.

2. La manipulation psychologique

Les techniques de cette catégorie sont plus subtiles car, au lieu de modifier nos systèmes cognitifs, elles cherchent à exploiter ses faiblesses en tirant parti de nos biais cognitifs. Un biais cognitif est un mécanisme de la pensée qui dévie de la pensée rationnelle et qui fait porter des jugements ou prendre des décisions sans tenir compte d'un raisonnement analytique.

Il existe globalement différents biais cognitifs comme les biais qui découlent d'une saturation d'informations, d'informations incomplètes ou vagues, de la nécessité d'agir rapidement et des limites de la mémoire.

L'exemple suivant illustre comment les biais liés à la « nécessité d'agir rapidement » peuvent être exploités par un site marchand, ici [expedia.com](https://www.expedia.com). En affichant le message *In high demand – We have 1 left* (« Très demandé – seulement un seul restant »), le site donne l'impression que le produit est très recherché et risque de ne plus être disponible rapidement. L'utilisateur est alors incité à finaliser son achat, sans trop réfléchir.

Room Type	Sleep
> Double Room  Someone just booked this  In high demand - only 3 rooms left on our site 1 double bed   Private bathroom  Flat-screen TV  Soundproofing • Shower • Safety Deposit Box • TV • Telephone • Hairdryer • Iron • Radio • Desk • Free toiletries • Fan • Toilet • Heating	  J S 1

Ces manipulations peuvent exploiter des biais génériques ou ciblés pour chaque personne. En effet, même si nous sommes tous vulnérables aux biais cognitifs, les biais auxquels nous sommes le plus sensibles dépendent essentiellement de notre profil psychologique. Une attaque de manipulation pourrait donc être optimisée en fonction du profil psychologique de la cible.

La construction d'un profil psychologique peut reposer sur le modèle OCEAN⁶ qui évalue, pour chaque personne, les cinq facteurs suivants :

- (O) Ouverture d'esprit : tendance à être ouvert aux expériences nouvelles ;
- (C) Conscienciosité : tendance à être prudent, vigilant et consciencieux ;
- (E) Extraversion : tendance à chercher la stimulation, l'attention et la compagnie des autres ;
- (A) Agréabilité : tendance à être compatissant et coopératif plutôt que soupçonneux et antagonique envers les autres ;
- (N) Neuroticisme : tendance persistante à l'expérience des émotions négatives (anxiété, colère, culpabilité, déprime, etc.).

Ces profils sont établis en analysant les réponses données par la cible à une longue liste de questions telles que : « *Croyez-vous en l'importance de l'art ?* » ou « *Avez-vous régulièrement des moments de déprime ?* ». Il s'agit donc d'une tâche laborieuse, nécessitant la coopération des cibles et pouvant difficilement être mise en œuvre à grande échelle.

UNE ATTAQUE DE MANIPULATION POURRAIT DONC ÊTRE OPTIMISÉE EN FONCTION DU PROFIL PSYCHOLOGIQUE DE LA CIBLE

Cependant, une équipe de l'université de Cambridge a récemment démontré qu'il était possible d'établir le profil psychologique d'un ou d'une internaute uniquement en analysant ses *likes* sur Facebook⁷. Plus spécifiquement, ces travaux ont montré que 250 *likes* suffiraient pour obtenir un profil aussi précis que celui établi par son époux (ou épouse). Il est donc envisageable d'établir des profils psychologiques très précis, à grande échelle, en utilisant des plateformes comme Facebook, et cela complètement à l'insu des cibles.

250 LIKES SUFFIRAIENT POUR OBTENIR UN PROFIL PRÉCIS

Ce sont d'ailleurs ces résultats que l'entreprise Cambridge Analytica aurait utilisés lors de la campagne présidentielle de Donald Trump pour cibler les électeurs indécis et influençables. La plateforme de

Facebook est idéale pour ce type de ciblage et de manipulation, car elle permet à tout annonceur de définir des critères très fins (comme le niveau d'éducation, de revenus, les centres d'intérêt, les lieux géographiques, etc.). Ces critères peuvent, sans aucun doute, être choisis pour cibler différents profils psychologiques sans avoir à collecter les données personnelles. Les rôles sont bien partagés. L'annonceur définit les critères de ciblage et les messages à transmettre. Facebook a la charge, en utilisant toutes les données personnelles qu'elle possède, d'identifier les personnes à cibler et de leur transmettre les annonces.

3. La manipulation de type *dark pattern*

La dernière catégorie de manipulation consiste non pas à influencer la décision d'un utilisateur, mais de piéger l'utilisateur ou de lui faire faire des choses contre sa volonté. Les exemples de manipulation de ce type sont les attaques d'ingénierie sociale ou de *phishing*, qui induisent la victime en erreur et l'incitent à faire des choses qu'elle ne souhaite pas, ou des schémas sombres (*dark patterns*) qui trompent les utilisateurs en créant certaines tâches telles que l'accès à un menu de configuration, rendu artificiellement difficile à utiliser, comme l'illustre le schéma suivant.



Exemple de *dark pattern*

Pourquoi déclarez-vous craindre davantage la surveillance commerciale que la surveillance gouvernementale ? Expliquez-nous la réalité de la « dataveillance » ou « surveillance liquide » ?

LA PLATEFORME DE FACEBOOK EST IDÉALE POUR CE TYPE DE CIBLAGE et de manipulation

Je crains toutes les formes de surveillance de masse, qu'elles soient gouvernementales ou commerciales. Je voulais uniquement dire que j'ai l'impression que les médias se focalisent principalement sur la surveillance gouvernementale et pas assez sur la surveillance commerciale. On a beaucoup parlé des révélations de Snowden, mais on parle très peu des *data brokers*. La surveillance commerciale mériterait davantage d'attention de la part des médias. Ainsi, le grand public devrait être informé que nos données sont vendues aux enchères par les systèmes de RTB (*Real Time Bidding*)⁸, comme tout autre produit financier.

NOS DONNÉES SONT COLLECTÉES, ÉCHANGÉES, VENDUES DANS UNE OPACITÉ TOTALE

Nos données sont collectées, échangées, vendues dans une opacité totale. Le marché des données personnelles est tellement important, et les entreprises qui en vivent sont tellement puissantes, qu'il devient difficile de le contrôler et de le limiter. Les systèmes de profilage sont de plus en plus efficaces et furtifs. Par exemple, la technique de profilage « par empreintes » (*fingerprints*) des applications ou des appareils est complètement invisible et, par conséquent, indétectable. Elle utilise une combinaison d'attributs techniques d'un appareil, qui peuvent être facilement récoltés par les sites web, tels que la version du navigateur, le système d'exploitation, la taille de l'écran, ou la langue du navigateur pour en calculer une empreinte de l'appareil. Comme le montre l'article «Beauty and the Beast : Diverting modern web browsers to build unique browser fingerprints⁹» qui a obtenu le prix Cnil-Inria 2018¹⁰, cette technique est particulièrement efficace, car il existe une telle diversité d'appareils, mobiles ou fixes, connectés sur le web qu'il est souvent possible d'identifier un utilisateur de façon unique et ainsi d'identifier les pages qu'il visite.

Un autre exemple de dérive de la surveillance commerciale est Facebook. Ce réseau social vend un service de micro-ciblage ultraperformant. Ce service est utilisé par des publicitaires pour vendre des produits ou services, ou par des partis politiques. Facebook utilise pour cela les données et les métadonnées de la plateforme, mais aussi des données qu'elle collecte ou achète à des *data brokers*. Ce ciblage est si fin et si précis qu'il permet de faire du profilage psychologique utilisé à des fins de manipulation, comme dans l'affaire Cambridge Analytica. Ces manipulations peuvent influencer les résultats d'une élection et peuvent donc avoir un impact important sur la démocratie. De plus, alors qu'il y a seulement quelques dizaines

d'années les campagnes de propagande étaient réservées aux États qui en avaient les moyens, quelques milliers d'euros suffisent aujourd'hui pour atteindre un nombre très élevé de personnes. Elles sont donc à la portée de toutes les bourses.

QUELQUES MILLIERS D'EUROS SUFFISENT POUR ATTEINDRE UN NOMBRE TRÈS ÉLEVÉ DE PERSONNES

Facebook est devenu une arme de désinformation et de propagande très puissante. Il devrait être plus transparent sur les algorithmes employés pour cibler ses utilisateurs, mais aussi sur l'identité des entités qui en usent à des fins de ciblage.

La question de la régulation de ces plateformes se pose de plus en plus. Il conviendrait de réfléchir pour fixer des limites aux capacités du micro-ciblage. Les contenus de ces plateformes devraient être « modérés » afin de limiter la propagation des *fake news*. Cette modération soulève cependant des questions difficiles à résoudre. Par exemple : qui doit décider des règles de modération/filtrage ? Comment éviter le conflit entre modération des contenus et liberté d'expression ?

Pour revenir à votre question, il est intéressant de noter qu'il existe une vraie convergence entre la surveillance commerciale et la surveillance gouvernementale. Les gouvernements n'ont plus besoin de déployer leur propre système de surveillance. Les révélations Snowden ont bien montré que la NSA utilisait les données collectées par des entreprises privées pour mettre en place un système de surveillance de masse généralisée. Le système de « score social », mis en place par le gouvernement chinois, utilise également les données collectées par des entités privées. L'affaire Cambridge Analytica a aussi révélé que des gouvernements pouvaient utiliser des services privés – en l'occurrence Facebook –, pour déployer de vraies campagnes de propagande et de manipulation. La surveillance gouvernementale est donc de plus en plus sous-traitée par des entités privées.

La protection de la vie privée est-elle une chimère à l'heure de l'économie de la donnée personnelle ? Le RGPD est-il une bonne réponse ? Comment se prémunir contre une exploitation abusive des données personnelles ? La réponse serait-elle de nature technique, économique ou politique ?

il existe une vraie convergence entre la surveillance commerciale et la surveillance gouvernementale

Le RGPD (Règlement européen sur la protection des données) est une des réponses au problème. Il apporte de nouveaux éléments intéressants comme l'obligation d'effectuer une analyse d'impact, le droit à la

portabilité et des sanctions financières plus conséquentes. Force est de constater que les entreprises se préoccupent davantage de cette question depuis la mise en place de ce règlement.

On pourrait toutefois regretter que le « consentement » reste l'un des fondements juridiques privilégiés pour la collecte. Une entreprise peut donc souvent collecter toutes les données qu'elle souhaite si elle obtient le consentement de son émetteur. Cela explique pourquoi la plupart des sites web demande maintenant à leurs utilisateurs de cliquer sur une bannière pour les autoriser à collecter des données. Est-ce que cela a amélioré la situation pour les internautes ? Je ne sais pas. La plupart des internautes cliquent, par fatigue ou lassitude, sans vraiment consulter les politiques de *privacy*, qui de toute façon sont incompréhensibles pour la plupart d'entre nous. De plus, les entreprises sont très habiles pour obtenir ces fameux consentements, en utilisant notamment les fameux *dark patterns*¹¹.

Le RGPD est nécessaire, mais probablement pas suffisant. Il faut informer et éduquer les internautes pour qu'ils soient demandeurs de services plus respectueux de leur vie privée. Il faut aussi développer des services alternatifs plus protecteurs et montrer qu'ils sont économiquement viables. Le moteur de recherche Qwant est, à mon avis, un exemple à suivre... mais c'est compliqué de se battre contre des mastodontes comme Google.

Sources :

1. <https://www.inria.fr/equipes/privatics>
2. <https://www.scientificamerican.com/article/can-facebooks-machine-learning-algorithms-accurately-predict-suicide/>
3. <https://hal.inria.fr/hal-01419943>
4. <https://ieeexplore.ieee.org/document/6573302>
5. <https://www.wired.co.uk/article/china-social-credit-system-explained>
6. <https://www.ncbi.nlm.nih.gov/pubmed/1635039>
7. <https://www.pnas.org/content/112/4/1036>
8. <https://hal.inria.fr/hal-00915249/PDF/SellingOffPrivacyAtAuction.pdf>
9. <https://hal.inria.fr/hal-01285470v2>
10. <https://www.inria.fr/actualite/actualites-inria/remise-du-prix-Cnil-inria>
11. <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>

Categorie

1. Articles & chroniques

date créée

14 mars 2019

Auteur

claudecastel