La Â« datapulation Â» ou la manipulation par les donnÃ©es

Description

Interview de Claude Castelluccia – Propos recueillis par FranÃ§oise LaugÃ©e

Vous Ãªtes directeur de recherche Ã lâ€™Inria, sur quels sujets travaille actuellement lâ€™Ã©quipe appelÃ©e Privatics que vous dirigez ?

Lâ€™Ã©quipe Privatics[1]Â de lâ€™Inria (Institut national de recherche en informatique et en automatique) est localisÃ©e Ã Grenoble et Ã Lyon. Elle a pour objectif dâ€™Ã©tudier les nouvelles menaces qui pÃ¨sent sur la vie privÃ©e introduites par la sociÃ©tÃ© de lâ€™information et de concevoir des solutions prÃ©servant la vie privÃ©e. Nous travaillons sur des sujets aussi divers que lâ€™anonymisation des donnÃ©es, la protection de la vie privÃ©e dans lâ€™internet des objets, lâ€™analyse des systÃ¨mes de surveillance et de profilage ou la transparence des algorithmes et des systÃ¨mes.

Le projet suit une approche multidisciplinaire. Il se concentre sur des questions techniques et scientifiques, mais il prend Ã©galement en considÃ©ration les aspects Ã©conomiques, juridiques et sociaux de la vie privÃ©e. Nous collaborons notamment avec la Cnil (Commission nationale de l’informatique et des libertÃ©s) dans le cadre de la convention Cnil-Inria.

Pour ainsi dire, nous Â«Â payonsÂ Â», avec des informations qui relÃ¨vent de notre vie privÃ©e, lâ€™accÃ¨s Ã des services web personnalisÃ©s. Quel est le niveau de performance des techniques de profilage aujourdâ€™huiÂ ? Pour quels usagesÂ ? Et avec quels effets ?

CES TECHNIQUES Dâ€™ANALYSE PERMETTENT Dâ€™IDENTIFIER NOS Ã‰TATS Ã‰MOTIONNELS OU NOS PROFILS PSYCHOLOGIQUES

Nos donnÃ©es personnelles sont collectÃ©es et analysÃ©es par diverses entreprises ou entitÃ©s Ã des fins de personnalisation, catÃ©gorisation ou de surveillance. Ces techniques dâ€™analyse sont trÃ¨s puissantes et permettent, parmi dâ€™autres choses, dâ€™identifier nos Ã©tats Ã©motionnels ou nos profils psychologiques. Il a Ã©tÃ© montrÃ© que lâ€™analyse des donnÃ©es Facebook peut identifier prÃ©cocement les utilisateurs qui ont des tendances suicidaires[2].

Ces donnÃ©es sont collectÃ©es sur internet, lorsque nous visitons des sites web ou des rÃ©seaux sociaux, mais aussi dans le monde physique, grÃ¢ce Ã nos tÃ©lÃ©phones portables. Câ€™est ce quâ€™on appelle le Â«Â profilage physique[3]Â Â». En effet, les applications que nous utilisons sur nos tÃ©lÃ©phones

intelligents collectent de nombreuses donnÃ©es comportementales, qui permettent de nous gÃ©olocaliser. Cette gÃ©olocalisation sert, en outre, Ã identifier nos points dâ€™intÃ©rÃªt.

Ce profilage est essentiellement effectuÃ© par des entitÃ©s tierces Ã des fins de ciblage publicitaire ou de personnalisation de services. Il est Ã©galement utilisÃ© pour catÃ©goriser les comportements des utilisateurs. Ces informations sont trÃ¨s utiles, notamment pour les banques ou les assurances lorsquâ€™elles souhaitent proposer un service Ã un client. Il existe aussi un vrai marchÃ© des donnÃ©es, collectÃ©es par desÂ *data*Â *brokers*Â qui revendent ces donnÃ©es (voirÂ *La rem*Â nÂ°46-47, p.77). Finalement, ce profilage est Ã©galement utilisÃ© Ã des fins sÃ©curitaires, comme lâ€™ont montrÃ© les rÃ©vÃ©lations de Snowden sur la collecte de masse effectuÃ©e par la NSA[4].

CETTE GÃ‰OLOCALISATION SERT Ã€ IDENTIFIER NOS POINTS Dâ€™INTÃ‰RÃŠT

Les dangers de ce profilage sont multiples. Il permet de Â«Â catÃ©goriserÂ Â» les internautes, ce qui peut conduire Ã des risques de discrimination. Une assurance pourra dÃ©cider de ne pas assurer une personne si son profil correspond Ã un profil Â«Â Ã risqueÂ Â». Les risques et les dangers de ce type de catÃ©gorisation peuvent Ãªtre importants comme on peut le voir avec les systÃ¨mes de Â«Â police prÃ©dictiveÂ Â» ou de Â«Â score socialÂ Â» en Chine[5].

Un autre danger de ce profilage, et plus particuliÃ¨rement de lâ€™utilisation de ce profilage pour faire du ciblage, est ce quâ€™on appelle communÃ©ment la Â«Â bulle de filtresÂ Â» (*filter bubble*). La Â«Â bulle de filtresÂ Â» dÃ©signe l'Ã©tat dâ€™isolement intellectuel et culturel dans lequel un internaute se retrouve lorsque les informations qu'il reÃ§oit sur internet sont uniquement ciblÃ©es en fonction de son profil.

Quâ€™est-ce que la Â«Â datapulationÂ Â» (data et manipulation) et pourquoi dites-vous queÂ *Â«Â comme notre infrastructure Ã©nergÃ©tique, notre infrastructure cognitive est critiqueÂ Â»*Â ?

Comme nous lâ€™avons soulignÃ© prÃ©cÃ©demment, nos donnÃ©es personnelles sont utilisÃ©es Ã des fins de surveillance et de ciblage. La Â«Â dataveillanceÂ Â» (surveillance par les donnÃ©es) est la pratique qui consiste Ã collecter des donnÃ©es et des mÃ©tadonnÃ©es dans le but de surveiller des individus.

Ce que lâ€™on sait moins, câ€™est que nos donnÃ©es personnelles sont de plus en plus utilisÃ©es pour nous influencer, voire nous manipuler. Câ€™est ce que jâ€™appellerais la Â«Â datapulationÂ Â» (la manipulation par les donnÃ©es). En contrÃ´lant les informations que nous recevons en ligne et en les adaptant Ã nos comportements, un service comme Facebook peut Ãªtre utilisÃ© pour influencer nos comportements de clients, nos opinions, nos Ã©motions, voire, comme le suggÃ¨re lâ€™affaire rÃ©cente Â«Â Cambridge AnalyticaÂ Â», nos choix politiques (voirÂ *La rem*Â nÂ°48, p.90). Ces manipulations,

trÃ¨s Ã©tudiÃ©es en marketing comportemental (*neuromarketing*), sont les consÃ©quences mÃªme du modÃ¨le Ã©conomique de lâ€™internet et de ses services Â«Â gratuitsÂ Â». Il devient urgent de dÃ©velopper des solutions pour sâ€™en protÃ©ger et sÃ©curiser notre Â«Â infrastructure cognitiveÂ Â», qui est probablement au moins aussi critique que notreÂ infrastructureÂ Ã©nergÃ©tique ou de tÃ©lÃ©communication.

NOS DONNÃ‰ES PERSONNELLES SONT DE PLUS EN PLUS UTILISÃ‰ES POUR NOUS INFLUENCER, VOIRE NOUS MANIPULER

Les techniques de manipulation par les donnÃ©es sont nombreuses et variÃ©es. On peut cependant les classer en trois grandes catÃ©goriesÂ :

1. les techniques basÃ©es sur la Â«Â manipulation informationnelleÂ Â» ;
2. celles basÃ©es sur la Â«Â manipulation psychologique ou cognitiveÂ Â» ;
3. celles dont le but est de rendre lâ€™exÃ©cution dâ€™une action difficile ou de tromper lâ€™utilisateur, ce que lâ€™on appelle en anglais les *dark patterns*.

1. La manipulation informationnelle

Les techniques de cette catÃ©gorie tentent de modifier notre systÃ¨me cognitif en polluant les informations ou connaissances que nous utilisons pour le construire. Câ€™est typiquement le cas des fausses informations publiÃ©es sur le web ou les rÃ©seaux sociaux (lesÂ *fake news*), dont lâ€™objectif est dâ€™influencer nos opinions, et parfois nos votes.

IL DEVIENT URGENT DE SÃ‰CURISER NOTREÂ Â«INFRASTRUCTURE COGNITIVEÂ»

Dans un rapport rÃ©cent intitulÃ© Â«Â Information DisorderÂ : Toward an interdisciplinary framework for research and policy makingÂ Â» (voirÂ *La remÂ* nÂ°45, p.62), le Conseil de lâ€™Europe fait la distinction entre deux classes de publications dâ€™informations Â«Â nuisiblesÂ Â»Â :

- La dÃ©sinformation consiste Ã diffuser une information fausse dans le but de nuire (on parle alors de dis-information ouÂ *fake news* en anglais), ou par ignorance ou erreur (on parle alors de mal-information (*mis-information*Â en anglais). Un exemple de dis-information est lâ€™information, qui a circulÃ© pendant la campagne prÃ©sidentielle, prÃ©tendant faussement que la campagne du candidat Macron Ã©tait financÃ©e par lâ€™Arabie saoudite.
- La mal-information est une information correcte, souvent confidentielle ou privÃ©e, mais publiÃ©e

Ã grande Ã©chelle dans un but spÃ©cifique. Câ€™est lâ€™exemple des courriels privÃ©s, volÃ©s et publiÃ©s sur internet pendant la derniÃ¨re campagne prÃ©sidentielle aux Ã‰tats-Unis.

On peut Ã©galement ajouter Ã cette catÃ©gorie de manipulations les techniques de filtrage ou de censure de lâ€™information.

2. La manipulation psychologique

Les techniques de cette catÃ©gorie sont plus subtiles car, au lieu de modifier nos systÃ¨mes cognitifs, elles cherchent Ã exploiter ses faiblesses en tirant parti de nos biais cognitifs. Un biais cognitif est un mÃ©canisme de la pensÃ©e qui dÃ©vie de la pensÃ©e rationnelle et qui fait porter des jugements ou prendre des dÃ©cisions sans tenir compte dâ€™un raisonnement analytique.

Il existe globalement diffÃ©rents biais cognitifs comme les biais qui dÃ©coulent dâ€™une saturation dâ€™informations, dâ€™informations incomplÃ¨tes ou vagues, de la nÃ©cessitÃ© dâ€™agir rapidement et des limites de la mÃ©moire.

Lâ€™exemple suivant illustre comment les biais liÃ©s Ã la Â«Â nÃ©cessitÃ© dâ€™agir rapidementÂ Â» peuvent Ãªtre exploitÃ©s par un site marchand, ici expedia.com. En affichant le messageÂ *In high demand*Â â€“Â *We have 1 leftÂ* (Â« TrÃ¨s demandÃ© â€“ seulement un seul restantÂ Â»), le site donne lâ€™impression que le produit est trÃ¨s recherchÃ© et risque de ne plus Ãªtre disponible rapidement. Lâ€™utilisateur est alors incitÃ© Ã finaliser son achat, sans trop rÃ©flÃ©chir.

Exemple d'exploitation de biais cognitifs par un sit

Ces manipulations peuvent exploiter des biais gÃ©nÃ©riques ou ciblÃ©s pour chaque personne. En effet, mÃªme si nous sommes tous vulnÃ©rables aux biais cognitifs, les biais auxquels nous sommes le plus sensibles dÃ©pendent essentiellement de notre profil psychologique. Une attaque de manipulation pourrait donc Ãªtre optimisÃ©e en fonction du profil psychologique de la cible.

La construction dâ€™un profil psychologique peut reposer surÂ le modÃ¨leÂ OCEAN[6]Â qui Ã©value, pour chaque personne, les cinq facteurs suivants :

- (O)Â Ouverture dâ€™espritÂ : tendance Ã Ãªtre ouvert aux expÃ©riences nouvelles ;
- (C)Â ConscienciositÃ©Â : tendance Ã Ãªtre prudent, vigilant et consciencieux ;
- (E)Â ExtraversionÂ : tendance Ã chercher la stimulation, lâ€™attention et la compagnie des autres ;
- (A)Â AgrÃ©abilitÃ©Â : tendance Ã Ãªtre compatissant et coopÃ©ratif plutÃ´t que soupÃ§onneux et antagonique envers les autres ;
- (N)Â NeuroticismeÂ : tendance persistante Ã lâ€™expÃ©rience des Ã©motions nÃ©gatives (anxiÃ©tÃ©, colÃ¨re, culpabilitÃ©, dÃ©prime, etc.).

Ces profils sont Ã©tablis en analysant les rÃ©ponses donnÃ©es par la cible Ã une longue liste de questions telles queÂ :Â *Â«Â Croyez-vous en lâ€™importance de lâ€™artÂ ?Â Â»*Â ouÂ *Â«Â Avez-vous rÃ©guliÃ¨rement des moments de dÃ©primeÂ ?Â Â»*. Il sâ€™agit donc dâ€™une tÃ¢che laborieuse, nÃ©cessitant la coopÃ©ration des cibles et pouvant difficilement Ãªtre mise en Å“uvre Ã grande Ã©chelle.

UNE ATTAQUE DE MANIPULATION POURRAIT DONC ÃŠTRE OPTIMISÃ‰E EN FONCTION DU PROFIL PSYCHOLOGIQUE DE LA CIBLE

Cependant, une Ã©quipe de lâ€™universitÃ© de Cambridge a rÃ©cemment dÃ©montrÃ© quâ€™il Ã©tait possible dâ€™Ã©tablir le profil psychologique dâ€™un ou dâ€™une internaute uniquement en analysant sesÂ *likes*Â sur Facebook[7]. Plus spÃ©cifiquement, ces travaux ont montrÃ© que 250 *likes* Â suffiraient pour obtenir un profil aussi prÃ©cis que celui Ã©tabli par son Ã©poux (ou Ã©pouse). Il est donc envisageable dâ€™Ã©tablir des profils psychologiques trÃ¨s prÃ©cis, Ã grande Ã©chelle, en utilisant des plateformes comme Facebook, et cela complÃ¨tement Ã lâ€™insu des cibles.

250 LIKES SUFFIRAIENT POUR OBTENIR UN PROFIL PRÃ‰CIS

Ce sont dâ€™ailleurs ces rÃ©sultats que lâ€™entreprise Cambridge Analytica aurait utilisÃ©s lors de la campagne prÃ©sidentielle de Donald Trump pour cibler les Ã©lecteurs indÃ©cis et influenÃ§ables. La plateforme de Facebook est idÃ©ale pour ce type de ciblage et de manipulation, car elle permet Ã tout annonceur de dÃ©finir des critÃ¨res trÃ¨s fins (comme le niveau dâ€™Ã©ducation, de revenus, les centres dâ€™intÃ©rÃªt, les lieux gÃ©ographiques, etc.). Ces critÃ¨res peuvent, sans aucun doute, Ãªtre choisis pour cibler diffÃ©rents profils psychologiques sans avoir Ã collecter les donnÃ©es personnelles. Les rÃ´les sont bien partagÃ©s. Lâ€™annonceur dÃ©finit les critÃ¨res de ciblage et les messages Ã transmettre. Facebook a la charge, en utilisant toutes les donnÃ©es personnelles quâ€™elle possÃ¨de, dâ€™identifier les personnes Ã cibler et de leur transmettre les annonces.

3. La manipulation de type *dark pattern*

La derniÃ¨re catÃ©gorie de manipulation consiste non pas Ã influencer la dÃ©cision dâ€™un utilisateur, mais de piÃ©ger lâ€™utilisateur ou de lui faire faire des choses contre sa volontÃ©. Les exemples de manipulation de ce type sont les attaques d’ingÃ©nierie sociale ou deÂ *phishing*, qui induisent la victime en erreur et lâ€™incitent Ã faire des choses qu’elle ne souhaite pas, ou des schÃ©mas sombres (*dark patterns*) qui trompent les utilisateurs en crÃ©ant certaines tÃ¢ches telles que l’accÃ¨s Ã un menu de configuration, rendu artificiellement difficile Ã utiliser, comme lâ€™illustre le schÃ©ma suivant.

Exemple de *dark pattern*

source : http://colingray.me/wp-content/up
2018_Grayetal_CHI_DarkPatternsUXDesig

Pourquoi dÃ©clarez-vous craindre davantage la surveillance commerciale que la surveillance gouvernementale ? Expliquez-nous la rÃ©alitÃ© de la Â« dataveillance Â» ou Â«Â surveillance liquideÂ Â»Â ?

LA PLATEFORME DE FACEBOOK EST IDÃ‰ALE POUR CE TYPE DE CIBLAGe et de manipulation

Je crains toutes les formes de surveillance de masse, quâ€™elles soient gouvernementales ou commerciales. Je voulais uniquement dire que jâ€™ai lâ€™impression que les mÃ©dias se focalisent principalement sur la surveillance gouvernementale et pas assez sur la surveillance commerciale. On a beaucoup parlÃ© des rÃ©vÃ©lations de Snowden, mais on parle trÃ¨s peu desÂ *data*Â *brokers*. La surveillance commerciale mÃ©riterait davantage dâ€™attention de la part des mÃ©dias. Ainsi, le grand public devrait Ãªtre informÃ© que nos donnÃ©es sont vendues aux enchÃ¨res par les systÃ¨mes de RTB (*Real Time Bidding*)[8], comme tout autre produit financier.

NOS DONNÃ‰ES SONT COLLECTÃ‰ES, Ã‰CHANGÃ‰ES, VENDUES DANS UNE OPACITÃ‰ TOTALE

Nos donnÃ©es sont collectÃ©es, Ã©changÃ©es, vendues dans une opacitÃ© totale. Le marchÃ© des donnÃ©es personnelles est tellement important, et les entreprises qui en vivent sont tellement puissantes, quâ€™il devient difficile de le contrÃ´ler et de le limiter. Les systÃ¨mes de profilage sont de plus en plus efficaces et furtifs. Par exemple, la technique de profilage Â«Â par empreintesÂ Â» (*fingerprints*) des applications ou des appareils est complÃ¨tement invisible et, par consÃ©quent, indÃ©tectable. Elle utilise une combinaison dâ€™attributs techniques dâ€™un appareil, qui peuvent Ãªtre facilement rÃ©coltÃ©s par les sites web, tels que la version du navigateur, le systÃ¨me dâ€™exploitation, la taille de lâ€™Ã©cran, ou la langue du navigateur pour en calculer une empreinte de lâ€™appareil. Comme le montre lâ€™articleÂ Â«Beauty and the BeastÂ : Diverting modern web browsers to build unique bowser fingerprints[9]Â»Â qui a obtenu le prix Cnil-Inria 2018[10], cette technique est particuliÃ¨rement efficace, car il existe une telle diversitÃ© dâ€™appareils, mobiles ou fixes, connectÃ©s sur le web quâ€™il est souvent possible dâ€™identifier un utilisateur de faÃ§on unique et ainsi dâ€™identifier les pages quâ€™il visite.

Un autre exemple de dÃ©rive de la surveillance commerciale est Facebook. Ce rÃ©seau social vend un service de micro-ciblage ultraperformant. Ce service est utilisÃ© par des publicitaires pour vendre des produits ou services, ou par des partis politiques. Facebook utilise pour cela les donnÃ©es et les mÃ©tadonnÃ©es de la plateforme, mais aussi des donnÃ©es quâ€™elle collecte ou achÃ¨te Ã desÂ *data*

Â *brokers*. Ce ciblage est si fin et si prÃ©cis quâ€™il permet de faire du profilage psychologique utilisÃ© Ã des fins de manipulation, comme dans lâ€™affaire Cambridge Analytica. Ces manipulations peuvent influencer les rÃ©sultats dâ€™une Ã©lection et peuvent donc avoir un impact important sur la dÃ©mocratie. De plus, alors quâ€™il y a seulement quelques dizaines dâ€™annÃ©es les campagnes de propagande Ã©taient rÃ©servÃ©es aux Ã‰tats qui en avaient les moyens, quelques milliers dâ€™euros suffisent aujourdâ€™hui pour atteindre un nombre trÃ¨s Ã©levÃ© de personnes. Elles sont donc Ã portÃ©e de toutes les bourses.

QUELQUES MILLIERS Dâ€™EUROS SUFFISENT POUR ATTEINDRE UN NOMBRE TRÃˆS Ã‰LEVÃ‰ DE PERSONNES

Facebook est devenu une arme de dÃ©sinformation et de propagande trÃ¨s puissante. Il devrait Ãªtre plus transparent sur les algorithmes employÃ©s pour cibler ses utilisateurs, mais aussi sur lâ€™identitÃ© des entitÃ©s qui en usent Ã des fins de ciblage.

La question de la rÃ©gulation de ces plateformes se pose de plus en plus. Il conviendrait de rÃ©flÃ©chir pour fixer des limites aux capacitÃ©s du micro-ciblage. Les contenus de ces plateformes devraient Ãªtre Â«Â modÃ©rÃ©sÂ Â» afin de limiter la propagation desÂ *fake news*. Cette modÃ©ration soulÃ¨ve cependant des questions difficiles Ã rÃ©soudre. Par exempleÂ : qui doit dÃ©cider des rÃ¨gles de modÃ©ration/filtrageÂ ? Comment Ã©viter le conflit entre modÃ©ration des contenus et libertÃ© dâ€™expressionÂ ?

Pour revenir Ã votre question, il est intÃ©ressant de noter quâ€™il existe une vraie convergence entre la surveillance commerciale et la surveillance gouvernementale. Les gouvernements nâ€™ont plus besoin de dÃ©ployer leur propre systÃ¨me de surveillance. Les rÃ©vÃ©lations Snowden ont bien montrÃ© que la NSA utilisait les donnÃ©es collectÃ©es par des entreprises privÃ©es pour mettre en place un systÃ¨me de surveillance de masse gÃ©nÃ©ralisÃ©e. Le systÃ¨me de Â«Â score socialÂ Â», mis en place par le gouvernement chinois, utilise Ã©galement les donnÃ©es collectÃ©es par des entitÃ©s privÃ©es. Lâ€™affaire Cambridge Analytica a aussi rÃ©vÃ©lÃ© que des gouvernements pouvaient utiliser des services privÃ©s â€“ en lâ€™occurrence Facebook â€“, pour dÃ©ployer de vraies campagnes de propagande et de manipulation. La surveillance gouvernementale est donc de plus en plus sous-traitÃ©e par des entitÃ©s privÃ©es.

La protection de la vie privÃ©e est-elle une chimÃ¨re Ã lâ€™heure de lâ€™Ã©conomie de la donnÃ©e personnelle ? Le RGPD est-il une bonne rÃ©ponse ? Comment se prÃ©munir contre une exploitation abusive des donnÃ©es personnelles ? La rÃ©ponse serait-elle de nature technique, Ã©conomique ou politique ?

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

Le RGDP (RÃ¨glement europÃ©en sur la protection des donnÃ©es) est une des rÃ©ponses au problÃ¨me. Il apporte de nouveaux Ã©lÃ©ments intÃ©ressants comme lâ€™obligation dâ€™effectuer une analyse dâ€™impact, le droit Ã la portabilitÃ© et des sanctions financiÃ¨res plus consÃ©quentes. Force est de constater que les entreprises se prÃ©occupent davantage de cette question depuis la mise en place de ce rÃ¨glement.

On pourrait toutefois regretter que le Â«Â consentementÂ Â» reste lâ€™un des fondements juridiques privilÃ©giÃ©s pour la collecte. Une entreprise peut donc souvent collecter toutes les donnÃ©es quâ€™elle souhaite si elle obtient le consentement de son Ã©metteur. Cela explique pourquoi la plupart des sites web demande maintenant Ã leurs utilisateurs de cliquer sur une banniÃ¨re pour les autoriser Ã collecter des donnÃ©es. Est-ce que cela a amÃ©liorÃ© la situation pour les internautesÂ ? Je ne sais pas. La plupart des internautes cliquent, par fatigue ou lassitude, sans vraiment consulter les politiques deÂ *privacy*, qui de toute faÃ§on sont incomprÃ©hensibles pour la plupart dâ€™entre nous. De plus, les entreprises sont trÃ¨s habiles pour obtenir ces fameux consentements, en utilisant notamment les fameuxÂ *dark patterns*[11]Â .

Le RGPD est nÃ©cessaire, mais probablement pas suffisant. Il faut informer et Ã©duquer les internautes pour quâ€™ils soient demandeurs de services plus respectueux de leur vie privÃ©e. Il faut aussi dÃ©velopper des services alternatifs plus protecteurs et montrer quâ€™ils sont Ã©conomiquement viables. Le moteur de recherche Qwant est, Ã mon avis, un exemple Ã suivreâ€¦ mais câ€™est compliquÃ© de se battre contre des mastodontes comme Google.

SourcesÂ :

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

Â
Categorie

1. Articles & chroniques

date crÃ©Ã©e
14 mars 2019
Auteur
claudecastel