

Traduction de l'expression anglophone *social cooling*, ce concept a été inventé par le Néerlandais Tijmen Schep, critique des technologies, *privacy designer* et spécialiste des questions d'éthique en matière d'innovation. « Le refroidissement social » désigne la retenue que chacun exercerait dans ses activités en ligne, allant jusqu'à une forme d'autocensure afin de préserver sa réputation. De plus en plus conscients des effets pervers liés à l'exploitation commerciale des traces qu'ils laissent sur le Net, les internautes seraient amenés à jouer au modérateur pour eux-mêmes, en contrôlant les contenus qu'ils postent ou qu'ils partagent, voire leurs simples recherches ou utilisations des services de l'internet, afin que leur vie numérique n'entache pas leur image dans la vie réelle.

Sur la page d'accueil du site web [Socialcooling](#), lancé en 2017 et consacré à ce phénomène, Tijmen Schep annonce que « *tout comme le pétrole conduit au réchauffement climatique, les données conduisent au refroidissement social* ». Autrement dit, à l'instar de la pollution atmosphérique, explique-t-il, le refroidissement social n'est pas un phénomène immédiatement perceptible mais la prise de conscience de ses effets néfastes pour la société est l'affaire de tous. Et nous devrions être plus prompts à réagir pour défendre une approche raisonnable et réfléchie de la vie privée, que nous l'avons été pour lutter contre la pollution de l'air que nous respirons.

Le chercheur néerlandais part du constat que, se sentant observé, chacun de nous va inévitablement changer son comportement, réflexe que « *le Big Data amplifie à l'extrême* » et qui pourra entraîner à long terme « *un gel de toute la société* ». Nous serions, selon lui, entrés subrepticement dans l'ère de l'économie de la réputation où chaque vie intime ou professionnelle fait l'objet d'une évaluation et se déroule au risque de cette évaluation ou notation. L'économie des données « *endommage l'environnement social* », prévient Tijmen Schep.

Une fois collectées, nos données personnelles, de toute nature, issues de nos agissements en ligne et hors ligne, font l'objet d'un traitement par des algorithmes programmés pour établir des catégories, des tendances et des modèles (*patterns*) offrant une représentation du corps social. Ainsi, les courtiers en données, ou *data brokers*, entreprises qui vivent de la revente de données dérivées, évaluent la probabilité que nous appartenions à tel ou tel profil, à partir des traces apparemment insignifiantes que nous avons laissées sur le Net, des « détails » concernant nos vies que nous n'avons nous-mêmes jamais divulgués. Le site Socialcooling en propose une liste édifiante : « *religion, victime de viol, fait un régime, aime le jardinage, nombre d'amis en ligne, nombre d'amis réel, QI, opinions politiques, a avorté, crédulité, orientation sexuelle projetée, orientation sexuelle réelle, lit des magazines de voyage, lit des livres de voyage, envisage d'avoir un enfant, parents divorcés avant ses 21 ans, névrosé(e), ouverture d'esprit, date de naissance, aime la mode, a des plantes à la maison, situation économique stable, héritier(ière) potentiel(le), extraverti(e), gentillesse, année de construction de la maison, fume à la maison, a des besoins de "senior", diabétique, a des tendances addictives, physiquement fragile, appareil de communication de prédilection, adulte sans enfant, niveau d'éducation, aime les articles commémoratifs d'Elvis* ». Et Tijmen Schep d'expliquer : « *Leurs "données dérivées" ont plus de valeur que "vos données"* ».

S'il vous disent qu'ils ne vendent pas vos données, demandez-leur s'ils vendent les leurs ».

Outre la question de la pertinence des modèles identifiés, liée notamment à la fiabilité des données collectées et aux biais inhérents à toute formule algorithmique, la manipulation de ces fameuses « données dérivées » peut se révéler préjudiciable pour les personnes concernées. « *Vous pouvez ne pas obtenir l'emploi de vos rêves si vos e-mails et vos publications Facebook ne sont pas assez positifs* » ; « *Si vous êtes une femme, vous pourriez avoir moins d'offres pour des emplois à forte rémunération* » ; « *Si vous avez de "mauvais amis" sur les réseaux sociaux, vous pourriez avoir à payer votre crédit plus cher* » : ce sont là autant d'exemples d'interprétations préjudiciables présentés sur le site Socialcooling.

Conscients du risque d'entrave à nos choix et à notre liberté en général, nous serions obligés de nous conformer à une « bonne » réputation en ligne, en adaptant nos comportements afin de ne pas être « mal jugés ». Tijmen Schep y décèle les effets pervers d'une société dessinée par le [Big Data](#), qui se résument selon lui en trois caractéristiques :

- Une culture du conformisme, soit l'effet de dissuasion provoqué par la crainte qu'une activité en ligne puisse être retenue en notre défaveur, aussi anodine soit-elle *a priori*. « *L'ironie : on ne nous enlève pas des libertés, on a juste peur de les utiliser* », analyse Tijmen Schep.
- Une culture d'évitement du risque, avec l'exemple de la notation des médecins new-yorkais. Une décision administrative a eu pour effet d'attribuer une plus mauvaise note à ceux qui soignaient des patients très malades car ils obtenaient un taux de mortalité plus élevé que ceux qui ne s'en occupaient pas et qui par conséquent étaient mieux notés.
- Une rigidité sociale accrue, lorsque « *les systèmes de réputation numérique limitent notre capacité et notre volonté de contester l'injustice* », citant la volonté des autorités chinoises de mettre en place, d'ici à 2020, un système de « crédit social » selon lequel les citoyens se verront attribuer des points, notamment en fonction de leur comportement et de leurs activités en ligne, leur score sera déterminant pour accéder à leurs demandes (emploi, logement, école, prêt...). « *La pression sociale est la plus forte et la plus subtile des formes de contrôle* », explique Tijmen Schep.

COURTIERS EN DONNÉES (DATA-BROKERS)

Acteurs majeurs de l'économie du *Big Data*, ces entreprises ont pour activité d'agréger, combiner, analyser, louer ou revendre les données personnelles des consommateurs, après traitement, et cela par milliards.

Une fois analysées et croisées avec de multiples autres sources publiques ou privées, les données brutes extraites des comportements numériques sont transformées et ainsi monnayées en tant que « données dérivées ».

Cette activité de courtage, traditionnelle dans le commerce des matières premières céréalières ou énergétiques, a pris une dimension particulière dans le secteur de l'information (au sens large du terme) avec l'essor du *Big Data*. Au cœur de l'économie des données, ces entreprises jouent le rôle d'intermédiaire en apportant de la valeur au « capital de données » collecté par les uns et en le revendant aux autres pour développer leur activité.

Outre les plateformes numériques, au premier rang desquelles Google et Facebook, de nombreux secteurs sont également impliqués dans le profilage des consommateurs, tels que le commerce de détails, les médias, l'édition, les télécommunications, les fabricants ou fournisseurs de terminaux, les banques, les assurances... S'y ajoutent les administrations publiques et les services en commun comme l'éducation, la santé, le logement, les transports, l'énergie, les allocations, la sécurité nationale... L'activité de partage ou de vente des données personnelles implique un grand nombre d'acteurs privés et publics.

Sociétés privées, les courtiers en données, n'étant pas en relation directe avec les consommateurs, restent inconnus de ceux-ci. Détenant chacune des milliards d'informations sur plusieurs centaines de millions de personnes, ces revendeurs de données ont pour nom Acxiom, leader au niveau mondial, Experian, Epsilon, Equifax, Nielsen, Oracle Data Cloud, TransUnion, WPP PLC ou encore Cambridge Analytica (au cœur du scandale du vol des données de 87 millions de membres du réseau Facebook, voir *infra*). Ils opèrent dans le monde entier sur un marché d'une valeur supérieure à 150 milliards d'euros par an.

Les grandes plateformes en ligne telles que Google et Facebook sont aujourd'hui les acteurs les plus performants en matière de collecte d'informations sur la vie quotidienne en temps réel de milliards de personnes dans le monde. Néanmoins, elles ne vendent ni ne partagent directement le profil de leurs consommateurs numériques avec des entreprises tierces. En revanche, elles permettent aux entreprises spécialisées dans l'agrégation des données personnelles d'utiliser ces données, à leur propre bénéfice ou à celui d'annonceurs afin d'affiner le ciblage publicitaire. Pour chaque publicité diffusée sur sa plateforme grâce aux données dérivées d'un courtier, Facebook reverse une commission à ce dernier.

Première mesure prise à la suite du scandale Cambridge Analytica, Facebook a décidé, fin mars 2018, d'interrompre ses partenariats avec les courtiers en données. Autre mauvaise nouvelle pour ce secteur jusqu'ici très prospère : l'entrée en vigueur du Règlement général pour la protection des données (RGPD, voir *La rem* n°42-43, p.21), le 25 mai 2018, devrait contraindre les courtiers en données à revoir leurs conditions de collecte des informations personnelles.

Sources :

- Corporate Surveillance in Everyday Life, Wolfie Christl, a report by Cracked Labs, crackedlabs.org, June 2017.
- « Facebook désactive les data brokers », Thomas Coëffé, Blogdumoderateur.com, 29 mars 2018.

Dans un article publié sur le site de *L'Obs* en juillet 2017, la journaliste Émilie Brouze rappelle que l'idée d'un « *refroidissement social* » n'est pas nouvelle, signalant que diverses études ont déjà effectivement montré « les effets d'intimidation » (*chilling effects*) survenus à la suite des révélations de l'ancien consultant de la NSA, Edward Snowden, en 2013, qui ont démontré l'existence d'un système de surveillance de masse. Chercheur à l'université de Toronto, Jon Penney avait ainsi mis en lumière la baisse du nombre de consultations d'articles dans la version anglophone de Wikipédia faisant allusion, d'une façon ou d'une autre, au terrorisme dans les deux mois qui ont suivi. Le constat est le même pour des requêtes effectuées dans le moteur de recherche Google à partir de mots-clés « sensibles ». Les travaux de recherche de l'Américaine Elizabeth Stoycheff ont également contribué à démontrer un phénomène d'autocensure lié à la révélation de programmes de surveillance en ligne, agissant au détriment des opinions minoritaires.

Face aux algorithmes qui servent à évaluer nos moindres faits et gestes, Tijmen Schep défend l'idée que « *la vie privée, c'est avoir le droit d'être humain* ». Il s'interroge sur le risque à devenir « *plus raisonnables, mais moins humains* » ou encore « *trop transparents* » pour laisser émerger les différences et les points de vue minoritaires.

Cependant la propagation des *fake news* et autres discours débridés sur le Net ne laisse pas apparaître le moindre refroidissement social, contredisant ainsi la thèse soutenue par Tijmen Schep. Il en va de même de la grande insouciance avec laquelle la grande majorité des internautes inscrits sur les réseaux sociaux y publient des pans entiers de leur vie privée, sans s'inquiéter outre mesure de l'usage qui en sera fait. À l'inverse, d'autres pratiques en ligne, s'appuyant sur un système de notation comme les sites Airbnb ou Uber, fonctionnent assurément sur la base d'une autocensure, destinée à rester bien noté par les uns et par les autres, afin de continuer à exercer ou à bénéficier pleinement de ces services. Mais là encore, s'agit-il vraiment d'un refroidissement social ?

La prise de conscience du déploiement de l'économie des données est loin d'être généralisée et cela pour une simple raison, l'accès aux services en ligne gratuits s'étant fait, dès l'origine, grâce à la délivrance implicite par les utilisateurs de l'autorisation à exploiter leurs données. Mais nous avons changé d'échelle de mesure, avec un niveau de collecte et des possibilités de calcul, jamais atteints, ce qu'atteste en quelque sorte la nécessité de l'adoption (tardive) du Règlement général sur la protection des données (RGPD). Et pourtant cette nouvelle ère du *Big Data*, qui s'appuie sur la surveillance omniprésente des consommateurs, ne fait que commencer. D'ores et déjà étant tous concernés, notre dilemme s'accroîtra sans cesse entre notre désir de protéger notre vie privée et celui de profiter des outils de la modernité. L'informatique ambient, avec le déploiement des interfaces connectées permettant la surveillance, la mesure de nos gestes et de nos émotions, de manière transparente, à partir de technologies comme l'*eye tracking*, la reconnaissance faciale et les *wearables technologies* ou les futures interfaces homme-machine capables de retranscrire nos pensées, risque effectivement de nous rendre à ce point transparents que seule une forme d'auto-contrôle pourrait, peut-être, nous préserver à l'avenir des effets induits par une

automatisation omnisciente fonctionnant à partir de nos données personnelles.

Sources :

- Socialcooling.fr
- « Sur internet, vous sachant surveillé, vous n'êtes plus vous-même », Emilie Brouze, nouvelobs.com, 26 juillet 2017.