Gouvernance algorithmique: Vie privée et autonomie individuelle à l'ère des Big Data

Primavera de Filippi

Gouvernance algorithmique:
Vie privée et autonomie individuelle à l'ère des Big Data

Primavera De Filippi

CERSA - CNRS - Université Paris II

Berkman Center for Internet & Society at Harvard Law School

Résumé:
Les Big data se réfèrent à la collecte et à l'agrégation de grandes masses de données provenant de différentes sources, en vue d'en tirer des informations par l'intermédiaire d'analyses statistiques, descriptives et prédictives. L'analyse des données repose sur des techniques de 'data mining' qui consistent à agréger des données apparemment sans rapport afin de trouver des modèles et des corrélations, extraire de nouvelles informations et parfais même prédire certains événements ou tendances.
Cet article examine les implications des Big data en ce qui concerne non seulement la vie privée des internautes mais aussi l'autonomie des individus. Aujourd'hui, de nombreux opérateurs en ligne se servent des Big data afin de fournir un service plus personnalisé à leur base d'utilisateurs, en fonction de leurs préférences (implicitement ou explicitement communiquées), leurs comportements passés et leurs communications en ligne. Ces pratiques —dénommées de "gouvernance algorithmique"— présentent un certain nombre d'avantages pour les utilisateurs, qui peuvent désormais profiter d'un service qui répond mieux à leurs attentes personnelles. Mais tandis que les avantages de la gouvernance algorithmique sont évidents pour la plupart des individus (qui donnent ainsi leur consentement pour la collecte et le traitement de leurs données personnelles), seuls quelques-uns d'entre eux réalisent effectivement le prix et les implications que cela peut avoir sur leur vie quotidienne.
À ce propos, cet article examine les obligations légales et morales auxquelles les fournisseurs de services en ligne devraient être soumis, étant donné l'énorme influence qu'ils ont sur leurs utilisateurs, et, par extension, la société en général. En particulier, à l'ère des Big data, le coût de la gouvernance algorithmique peut devenir très élevé. Un effort excessif de personnalisation excessive pourraient éventuellement se transformer en surveillance de masse et manipulation.
L'article conclut en montrant comment chaque décision déléguée à un algorithme constitue non seulement une menace pour le droit à la vie privée, mais aussi une restriction sur la capacité d'un individu à agir selon sa propre volonté.

Mots-clés: *gouvernance algorithmique, big data, surveillance, vie privée, autonomie*

Présentation

Les Big data se réfèrent à la collecte et l'agrégation de grandes masses de données produites par différentes personnes, choses ou interactions —y compris des données provenant des historiques de navigation, des forums Internet, des médias sociaux, des dossiers de santé, des archives gouvernementaux, etc. Dans la société de l'information, alors que la quantité de données produites ou collectées ne cesse de croître (Swan, 2012), leur agrégation et potentiels usages vont graduellement affecter de nombreuses facettes de notre vie. Mais les Big Data ne se réfèrent pas seulement au *volume* des données, ils se réfèrent aussi à la *variété* de ces données (qui diffèrent dans leur nature, source ou format), et à la *vitesse* croissante à laquelle elles sont produites et transférée dans le réseau —un modèle défini par Doug Laney (2012) comme les 3V des Big data. Avec l'arrivée de l'informatique en nuage (*cloud computing*), des centres de données spécialisés avec de fortes capacités de calcul permettent de traiter et d'analyser des quantités gigantesques de données provenant d'une variété de sources différentes (Lazar, 2012). L'analyse de ces données est d'autant plus précieuse qu'elle permet l'identification de modèles et de corrélations entre différents jeux de données, afin de pouvoir déduire de nouvelles informations, prévoir des comportements et évaluer la probabilité de certain événement (Franks, 2012). Ainsi, la poussée des Big data vont rapidement transformer la façon dont la plupart des individus agissent et interagissent entre eux (Mayer-Schönberger et Cukier, 2013), avec des répercussions aussi bien positives que négatives sur la société dans son ensemble (Bollier et Firestone, 2010).

Cet article ira explorer les obligations légales et morales des opérateurs en ligne qui se focalisent sur la collecte et le traitement de grandes masses de données, pour en analyser les implications potentielles sur la vie privée et l'autonomie des internautes. Après avoir exploré la relation entre personnalisation et vie privée (section I), l'article ira enquêter, d'une part, les bénéfices et les coûts liés à l'utilisation des Big data pour préserver l'ordre public, et d'autre part, les restrictions possibles sur les libertés civiles que cela pourrait entraîner (Section II).

Plus précisément, l'article analysera la mesure dans laquelle les opérateurs en ligne ont le droit d'utiliser les informations qu'ils détiennent à propos de leur base d'utilisateurs, lorsque ces informations ont été recueillies, déduites ou inférées à partir d'autres jeux de données. L'article ira questionner si les opérateurs en ligne qui ont accès à de grandes masses de données ont le droit et / ou l'obligation de divulguer des informations personnelles à des tiers, dès lors que cela serait nécessaire pour protéger le bien être personnel des individus (par exemple, en communiquant une maladie ou des tendances dépressives à un médecin) ou dans le but de préserver l'ordre public et la moralité (par exemple, en fournissant aux autorités publiques une liste de personnes profilées comme de potentielles menaces à la sécurité nationale). L'article se terminera par l'observation que si, d'une part, la gouvernance algorithmique permettrait l'établissement d'un environnement plus sûr et réglementé, elle pourrait également promouvoir la création d'un environnement oppressif et totalitaire, où la liberté d'actions des individus serait contrainte par la manière dont ils ont été profilés.

I. Un compromis entre personnalisation et vie privée

A. Big data et services personnalisés: une personnalisation guidée par les données

Aujourd'hui, les Big Data jouent un rôle important dans la définition des relations qui existent entre les citoyens et les institutions publiques ou les acteurs de marché. D'une part, la récente croissance en popularité des Big Data observée au cours des dernières années[1] est en train de transformer les opérations et les stratégies de marketing de nombreux acteurs commerciaux (LaValle & al., 2011) qui se focalisent sur la collecte et l'analyse des données provenant d'une variété de sources différentes afin à fournir des services plus personnalisés et mieux adaptés aux demandes de leurs clients. D'autre part, les opportunités fournies par le traitement de ces grandes masses de données sont également en train d'être appréhendées par la société civile et les institutions publiques, qui se concentrent de plus en plus sur des études statistiques et des analyses prédictives afin d'acquérir de nouvelles connaissances pour ce qui en est de l'environnement social, économique et politique global (Cukier & Mayer-Schoenberger, 2013).

Au niveau macro-économique, les données recueillies à partir de différentes sources (y compris les données publiques relatives à la démographie et à l'économie d'un pays, les infrastructures de l'espace public, tels que les bâtiments, les ponts et les autoroutes munis de capteurs, ou les dispositifs individuels tels que les ordinateurs, tablettes ou smart-phones) sont regroupées et traitées par des algorithmes sophistiqués afin d'obtenir des informations détaillées sur les grandes tendances économiques et sociales de notre société, qui constituent la base de nombreuses décisions commerciales et / ou politiques (Lohr, 2012). Il s'agit, par exemple, d'informations relatives aux débouchés commerciaux et aux perspectives futures d'activité, aux nouvelles opportunités en termes de mobilité sociale, aux niveaux de chômage prévisionnels, à la fluctuation des taux de criminalité, au besoin de renforcer les forces de sécurité, aux déficits potentiels pour les soins de santé, à l'avenir des épidémies et à la prévention des maladies, etc (Manovich, 2011).

Sur le plan micro-économique, les Big Data permettent aux institutions publiques et privées de mieux faire face (ou même d'anticiper) aux nouvelles opportunités d'innovation au niveau social, politique et économique (Simanis & Hart, 2012). Avec les Big data et les techniques de profilage modernes, ces institutions peuvent interagir avec les citoyens et les consommateurs sur un plan plus personnel, en utilisant les informations recueillies à leur sujet afin de fournir des services plus personnalisés qui sont susceptibles de répondre aux besoins et aux préférences spécifiques des individus. Ce résultat est obtenu par la collecte de grandes masses de données, pas seulement relatives aux *indicateurs démographiques* traditionnels (le sexe, l'âge, l'origine ethnique, la localisation géographique ou le revenu) mais aussi relatives à des indicateurs *psychographiques (i.e.* les traits de personnalité, les comportements, les attitudes, les aspirations ou tout autre

[1] Selon un rapport publié par International Data Corp. (2012), le marché des Big data dans le monde entier devrait passer de 3,2 milliards de dollars en 2010 à 16,9 milliards en 2015, avec un taux de croissance annuel composé (TCAC) de 40%.

critère de nature psychologique) qui caractérisent ces individus. Ces différents types de données peuvent ensuite être regroupés en grands jeux de données, et traitées par des algorithmes complexes et sophistiquées, afin de classer ces individus au sein de catégories spécifiques —des 'profiles'— qui détermineront la nature des interactions actuelles (et futures), ainsi que le type de services ou de contenus auxquels ces gens seront exposés.

Avec l''avènement des technologies numériques, l'effectivité et l'efficacité des Big Data ont considérablement augmenté, notamment en raison de la collecte massive de données et des nouvelles techniques d'analyse des pages Web, qui sont désormais devenues monnaie courante sur Internet. Tous les jours, de grandes masses de données —fournies, soit volontairement ou involontairement, par les internautes— sont recueillies par de nombreux opérateurs en ligne à des fins qui sont souvent difficiles à déterminer. La collecte de données est généralement justifiée par la nécessité de fournir des services personnalisés (*e.g*. dans le but de comprendre les goûts et les préférences des utilisateurs, d'améliorer la conception et les fonctionnalités de l'interface utilisateur, etc.), bien que la plupart des données collectées peuvent également être utilisé pour d'autres fins, moins légitimes, comme la surveillance ou de la publicité ciblée. Au-delà du profilage des internautes —à partir d'indicateurs démographiques et psychographiques— les opérateurs en ligne peuvent également collecter des données en temps réel sur les comportements et les communications en ligne de leur base d'utilisateurs, de manière à identifier des modèles qui pourront être utilisés pour obtenir des informations précises sur leur état d'esprit, tels que leur humeur ou leur état émotionnel (Bughin & al., 2011). Ainsi, les Big data bénéficient en fin de compte aussi bien les fournisseurs de services, qui peuvent bénéficier d'une meilleure compréhension de leur base d'utilisateurs, et les utilisateurs individuels qui peuvent bénéficier d'un service plus personnalisé. D'un point de vue commercial, notamment, les Big data sont intéressants dans la mesure où ils permettent aux fournisseurs de services d'afficher une publicité hautement personnalisés d'une manière qui est généralement invisible pour les consommateurs (Berry & Linoff, 2004). La plupart du temps, les Big Data sont également attrayant pour les utilisateurs, qui peuvent profiter de services qui sont parfaitement adaptés à leurs goûts et à leurs préférences personnelles, et qui peuvent évoluer au fil du temps afin de s'ajuster automatiquement à leurs besoins actuels.

Mais le potentiel réel des Big Data se réalise lorsque de multiples sources sont combinées en une seule grande base de données, qui sera traitée avec des algorithmes sophistiqués pour l'analyse de données (*data mining*) visant à extraire de nouvelles informations -grâce à des outils d'inférence statistique ou de déduction- qui n'étaient pas facilement accessibles à partir de chacun des jeux de données individuels (Cambria & al., 2013).

Cette tendance a commencé avec le mouvement de l'ouverture des données (Open Data), qui a démontré les avantages qui pourraient être tirés par la mise à disposition et la réutilisation des informations du secteur public (Davies, 2010). Plusieurs outils d'analyse et de visualisation des données ont été développés pour améliorer la lisibilité et l'intelligibilité de ces données, afin de promouvoir plus de transparence au sein du secteur public. Ces outils ont été rapidement adoptés par le secteur privé, en vue d'améliorer leurs stratégies de marketing basées sur l'analyse des

préférences des clients par l'intermédiaire des données comportementales (Richards & King, 2013). Bien que principalement déployée à des fins commerciales, l'adoption croissante Big data a montré qu'une valeur significative peut être extraite de la collection et de l'agrégation de grandes masses de données (souvent provenant de sources différentes) en un seul grand jeu de données. En effet, plus le jeu de données est important, plus il sera facile d'identifier des tendances et des corrélations (Lohr, 2012) afin de générer de nouvelles informations qui transmettront un nouveau sens à ce qui pourrait sembler autrement comme un tas de données déconnectées.

Aujourd'hui, le Big Data est considéré comme un "*buzz word*" qui s'est graduellement transformé en une vraie tendance (Swan, 2013). Comme illustré par la récente explosion des médias sociaux, les individus sont de plus en plus désireux de divulguer des informations sur eux-mêmes et sur le monde qui les entoure (Wolf, 2010). En agrégeant leurs propres données personnelles avec celles de leurs amis, ces individus peuvent acquérir de nouvelles connaissances au sujet de leur propre vie (ou celle de leurs amis) qu'ils pourraient autrement pas pu appréhender. Ainsi, le partage de données à caractère personnel est devenu une pratique de plus en plus commune, aussi bien dans le monde numérique que dans le monde physique. Cette tendance est particulièrement visible dans le contexte des communautés émergentes du *Quantified Self* (QS), caractérisées par une forte divulgation de données personnelles, souvent de nature très sensibles (telles que les données de santé). La récente croissance en popularité des dispositif qui supervisent l'activité des individus (comme le Fitbit, ou le Fuelband de Nike) et d'autres appareils d'auto-suivie (telles que les applications Zeo, MoodScope ou Momento, pour en citer quelques uns) n'est qu'un exemple de la façon dont les utilisateurs sont de plus en plus à l'aise avec la divulgation de leurs données personnelles, dans le but d'obtenir des informations plus personnalisées sur eux-mêmes, et de profiter d'un service plus personnalisé, qui s'adapte à leurs propres besoins.

B. Vie privée: la relation conflictuelle entre les Big data et la protection des données personnelles

Bien que les Big data fournissent des bénéfices importants aux internautes, la récolte massive des données en ligne et les techniques d'analyse des grandes masses de données, y compris les données personnelles ou sensibles, risquent de porter atteinte à certains droits fondamentaux. Bien que les internautes soient généralement au courant, et ont tendance à consentir à la collecte et au traitement de leurs données personnelles dans le but de recevoir un service plus personnalisé (Boyd & Crawford, 2012; Craig & Ludloff, 2012), il s'agit de comprendre la mesure dans laquelle ces pratiques pourraient, dans certains cas, porter atteinte au droit à la respect de la vie privée, énoncé à l'article 8 de la Charte européenne des droits de l'homme.

En Europe, la collecte et le traitement des données personnelles sont régis par la directive 95/46/CE (directive sur la protection des données personnelles) —qui sera bientôt remplacée par

le Règlement général sur la protection des données personnelles (GDPR)[2]—— et la directive 2002/58/CE sur la vie privée et les communications électroniques (directive ePrivacy) qui se concentre plus spécifiquement sur le traitement des données personnelles dans le secteur des communications électroniques.

L'article 7 de la directive sur la protection des données personnelles établit le principe de *l'opt-in,* selon lequel les données personnelles ne peuvent être traitées sans le consentement de la personne concernée, sauf si nécessaire pour préserver l'ordre public ou l'intérêt général de la société ou des individus. Se fondant sur ce principe, l'article 5 de la directive ePrivacy précise en outre que le traitement des données à caractère personnel ne peut être réalisé qu'avec le consentement de la personne concernée, qui doit avoir été informée de manière claire et complète en ce qui concerne la manière et le but du traitement des données (à moins que ce traitement ne soit directement connecté à la fourniture d'un service qui a été demandé explicitement par le sujet).

En fait, la plupart des internautes consentent à ce que leurs données personnelles soient collectées et traitées par des opérateurs en ligne, afin de bénéficier d'un service plus personnalisé qui ne serait pas possible autrement (Oboler, 2012). Or, le consentement est souvent obtenu par l'intermédiaire de conditions d'utilisation (Terms of Use) longues et complexes, que les utilisateurs sont souvent obligés à accepter afin de bénéficier des services offerts par ces opérateurs en ligne (Bradshaw et al., 2011). Les grands opérateurs, tels que Google ou Facebook, ont tendance à imposer unilatéralement les termes du contrat (qui peuvent donc être considérés comme des contrats d'adhésion)[3] de façon à favoriser leurs propres intérêts économiques, dans l'espoir que les internautes vont simplement accepter ces conditions, par nécessité ou l'indifférence. La plupart de ces condition d'utilisation sont souvent trop compliquées pour être correctement (ou totalement) comprises, et sont donc, souvent, tout simplement ignorées par les utilisateurs, qui finissent souvent par donner un consentement non informé au traitement de leurs données personnelles (Thompson, 2012).

Un autre problème critique pour la vie privée des internautes est dû au fait que les Big Data ne tiennent pas seulement compte des empreintes numériques laissées par les individus —c'est à

[2] L'objectif de la proposition de Règlement général sur la protection des données personnelles (GDPR) est celui d'harmoniser les réglementations au sein de l'Union Européeene, de manière à assurer une approche réglementaire plus cohérente qui soit capable de faire face aux récents développements technologiques tels que par exemple le cloud computing et les réseaux sociaux. Le premier projet de règlement a été publié le 25 Janvier 2012. Par la suite, de nombreux amendements ont été proposés par le Parlement européen et le Conseil des Ministres. Actuellement, le Conseil européen de l'UE vise doit encore adopter le règlement, qui devrait prendre effet après une période de transition de deux ans.

[3] Un contrat d'adhésion est défini comme «un accord juridiquement contraignant entre les deux parties du contrat, dans lequel un côté une des parties possède tout le pouvoir de négociation et l'utilise pour écrire le contrat principalement à son avantage. Un exemple de contrat d'adhésion sont toutes les formes normalisées de contrat qui offrent des biens ou des services aux consommateurs sur la base de conditions «à prendre ou à laisser», sans donner aux consommateurs la possibilité de négocier des conditions qui pourraient les bénéficier. Lorsque cela se produit, le consommateur ne peut pas obtenir le produit ou le service désiré à moins d'acquiescer au contrat." Source: West's Encyclopedia of American Law, edition 2. Copyright 2008 The Gale Group.

dire les traces qu'ils ont laissé derrière eux— mais aussi des *data shadows* —à savoir les informations relatives à certains individus qui ont été produites ou divulguées par d'autres (Koops 2011). Il arrive souvent, en particulier dans le contexte des réseaux sociaux, que des utilisateurs publient des informations non seulement sur eux-mêmes, mais aussi sur leurs amis ou personnes qui les entourent, généralement sans obtenir le consentement des personnes concernées. Ainsi, bien que tous les utilisateurs désireux de bénéficier des services offerts par certaines plates-formes en ligne (comme Google ou Facebook) doivent accepter les conditions d'utilisation des plates-formes concernées —consentant ainsi à ce que leurs données personnelles soient collectées et traitées par des opérateurs tiers— il est généralement impossible distinguer entre les informations fournies par un utilisateur qui ne concerne que lui, et celles qui contiennent également données personnelles relatives à des personnes tierces.

En outre, même en supposant que tous les utilisateurs aient réellement et consciemment consenti aux conditions d'utilisation d'une plate-forme donnée, par le simple fait d'agréger différents types de données en un seule grand jeu de données, les opérateurs en ligne peuvent déduire ou générer de nouvelles informations sur leur base d'utilisateurs (ou des tiers), qui vont souvent au-delà des informations qui ont été explicitement ou implicitement fournies par les utilisateurs eux-mêmes (Witten & Frank, 2005). Il devient donc de plus en plus difficile d'obtenir un consentement «informé», étant donné que les utilisateurs ne peuvent pas anticiper ce à quoi ils consentent, puisque les données ainsi déduites ou générées ne peuvent pas être a connues *a priori.*

À cet égard, l'analyse approfondie des données basée sur l'agrégation de multiples jeux de données provenant de différentes sources soulève une série de préoccupations en ce qui concerne le droit à l'anonymat ou le pseudonymat de certains individus désireux de maintenir une distinction entre leurs identités *online* et *offline*, ou même de ceux qui désirent adopter une identité différente selon les communautés avec lesquelles ils interagissent (Bus et Nguyen, 2013). Alors qu'il est souvent facile pour les opérateurs en ligne pour trouver une corrélation entre les différents profils d'utilisateurs (par exemple, parce qu'ils partagent un attribut commun tels que leur e-mail ou leur numéro de téléphone), certains utilisateurs pourraient être réticents à diffuser les informations qu'ils ont divulgué par rapport à l'une de leurs identités au-delà de la communauté dans laquelle ce profil était effectivement destiné à interagir.

Ceci est d'autant plus pertinent dans le contexte des grands jeux de données qui ont été délibérément «anonymisés» afin de se conformer aux règles sur la protection des données personnelles. En effet, si la plupart de ces règles ne s'appliquent qu'au traitement des données à caractère personnels —i.*e.* toutes données qui permettent l'identification d'une personne, directement ou indirectement, en vertu d'une de leurs caractéristiques distinctives[4]—— elles stipulent également que, afin d'établir si une personne peut effectivement être identifié à partir de ces données, il est nécessaire de prendre en compte tous les moyens disponibles au public pour

[4] Voir l'article 2 de la directive sur la protection des données personnelles, stipulant que «données personnelles» désigne toute information concernant une personne physique identifiée ou identifiable ("personne concernée"); une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs facteurs spécifiques à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

parvenir à une telle identification.[5] ”Ainsi, dans le cas des jeux de données qui ont été anonymisés, bien que l'identité des individus est efficacement protégé lorsque chaque jeu de données est considérée indépendamment, certains d'entre eux pourraient néanmoins être ré-identifiés par l'agrégation de plusieurs jeux de données dans un nouvel ensemble de données afin de trouver de nouveaux modèles et corrélations -une soi-disant “attaque d'inférence”.[6]

Comme la quantité de données collectées ne cesse de croître, il devient de plus en plus probable que les grands opérateurs en ligne, tels que Google, Facebook, ou Amazon finissent par devenir plus informés des intérêts et des préférences de leurs utilisateurs que les utilisateurs eux-mêmes (Cumbley & Church, 2013). Cela soulève, encore une fois, une série de problèmes par rapport au respect de la vie privée dans la mesure où, même si les utilisateurs ont effectivement consenti à la collecte et au traitement de certaines de leurs données personnelles, ils n'ont pas explicitement consenti à la collecte (ou, dans ce cas, à la production) et au traitement de l'information qui a été dérivée de ce processus (Kerr et Earle, 2013), et qui est également susceptible d'incorporer des données à caractère personnel. Les opérateurs en ligne ne devraient, par conséquent, pas pouvoir bénéficier du traitement de ces données sans le consentement préalable des personnes concernées. Or, étant donné que la plupart de ces traitements sont effectuées localement, et que les résultats ne sont pas accessibles au public mais uniquement utilisées en interne dans le seul but de fournir un service plus personnalisé, il est difficile pour les utilisateurs de réaliser que leur droit à au respect de la vie privée a effectivement été violé.

Plus grave encore, en dépit de l'amélioration croissante des outils statistiques et des algorithmes d'inférence, l'exactitude de l'information qui résulte de ce processus peut évidemment être remise en question (Kaisler, 2013). À cet égard, la directive sur la protection des données personnelles établit non seulement un droit pour les citoyens d'accéder à l'ensemble des données personnelles détenues par un tiers, et d'être informé de l'utilisation effective de celles-ci (article 12), elle leur permet aussi de s'opposer à une telle utilisation (article 14), ainsi que demander la rectification des données qu'ils considèrent inexactes (article 12). Or, étant donné que la plupart des individus ne sont pas au courant du fait que les opérateurs en ligne ont déduit des informations supplémentaires à leur sujet, ils est difficile pour ces derniers de s'opposer au traitement de ces données, et il leur est presque impossible de soumettre une demande pour que ces information soit, le cas échéant, rectifiées (Cavoukian & Jonas, 2012).

Cela est étroitement liée à la récente controverse autour du droit à l'oubli, consacré par l'article 17 du projet de règlement européen sur la protection des données personnelles,[7] qui reconnaît le droit pour chaque individu de *“déterminer le développement de sa vie de façon autonome, sans*

[5] Voir l'alinéa 26 de la directive sur la protection des données personnelles, stipulant que «les principes de la protection doivent s'appliquer à toute information concernant une personne identifiée ou identifiable; et que, pour déterminer si une personne est identifiable, il convient de tenir compte de tous les moyens susceptibles d'être raisonnablement utilisés par le contrôleur ou par toute autre personne pour identifier ladite personne ".

[6] Selon une étude effectuée par Golle (2006), le sexe, la date de naissance et code postal suffisent à identifier de manière unique plus de 87% de la population des États-Unis à partir de bases de données accessibles au public.

[7] European Commission. Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and On the Free Movement of Such Data (General Data Protection Regulation). 2012/0011 (COD). Article 17. Right to be forgotten and To Erasure

être perpétuellement ou périodiquement stigmatisé en conséquence d'une action spécifique réalisée dans le passé" (Mantelero, 2013). Bien que ce règlement sur la protection des données personnelles ne soit pas encore en vigueur, le droit à l'oubli a déjà été reconnu comme un droit fondamental par la Cour de justice européenne dans le cas *Costeja*,[8] où le tribunal a invoqué l'article 7 (respect de la vie privée et familiale) et l'article 8 (protection des données personnelles) de la Charte européenne des droits de l'homme pour demander à Google de retirer certaines informations à caractère personnel de ses résultats de recherche afin de se conformer à la législation européenne sur la protection des données personnelles. Jusqu'à présent, le droit à l'oubli a fait l'objet d'intenses critiques, en raison du fait que, après qu'une information a été rendue disponible sur Internet, il est pratiquement impossible pour le réseau de l'«oublier» (Weber, 2011; Rosen 2012 Stephens, 2014). En ce qui concerne, plus précisément, les problématiques de cet article, le droit à l'oubli est considérablement remis en cause par la montée en force des Big data. Comme l'a souligné l'Agence de sécurité de l'information du réseau européen (ENISA, 2012), les Big data pourrait produire des données statistiques (ou agrégées) contenant des informations qui —bien qu'elles n'aient jamais été divulguées— pourrait être extraite (ou désagrégées) par des mécanismes de *reverse-engineering,* en corrélant plusieurs jeux de données dérivés. Ainsi, bien que certaines informations ont été supprimées de la base de données d'origines, elles pourrait néanmoins être récupérés à une date ultérieure.

Par conséquent, même si une variété de règles sur la protection des données personnelles ont été adoptées pour protéger les individus contre la collecte, le traitement et l'utilisation non autorisée des données à caractère personnel, l'expansion rapide des Big Data est progressivement en train de rendre la plupart de ces lois obsolètes, non seulement parce que les utilisateurs sont de plus en plus disposés à donner leur consentement pour la collecte et le traitement de leurs données personnelles dans le but d'obtenir une plus grande personnalisation des produits offerts par des tiers, mais aussi parce que il est de plus en plus difficile pour les pouvoirs publics de faire respecter ces lois de la part des grands opérateurs en ligne qui opèrent dans un environnement transnational.

II. Le compromis entre l'ordre public et l'autonomie individuelle

A. Big data pour l'intérêt général: analyse descriptives et prédictives

Dans une société de plus en plus axée sur l'analyse des grandes masses de données, les bénéfices offerts par les Big data s'étendent bien au-delà des systèmes de recommandations ou des mécanismes de personnalisation visant à fournir un service plus adapté aux utilisateurs. Les techniques d'analyse et d'inférence statistique peuvent aussi être utilisés par les fournisseurs de services en ligne pour produire des informations qui pourraient potentiellement contribuer à la poursuite de l'intérêt général. L'information produite à partir de techniques de *data mining*

[8] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos*, Mario Costeja González (2014). Case C-131/12 of the Court of Justice of the European Union.

pourrait, en effet, fournir des indications utiles pour aborder de nombreuses questions importantes qui affectent actuellement les individus et la société dans son ensemble. Dans le secteur de la santé, les Big data peuvent entraîner d'importants progrès en matière de soins personnalisés, permettant d'améliorer le diagnostic des maladies et de réduire les coûts inutiles (Grove et al., 2013). Pour ce qui en est de l'application de la loi, les Big data pourraient soutenir les enquêtes de police, ou même directement contribuer à la prévention du crime en fournissant des informations aux autorités afin d'arrêter les criminels avant même qu'ils ne commettent un crime (Mancini et O'Reilly, 2013). D'un point de vue social, les Big data peuvent être utilisées pour mesurer le bien-être des différents quartiers de manière à identifier les secteurs soumis à une plus forte inégalité sociale (Joseph & Johnson, 2013). De même, en ce qui concerne la croissance économique, les Big data ont le potentiel d'accélérer le développement économique des pays émergents qui étaient traditionnellement affectés par des asymétries d'information fortes et un excessif manque de transparence (Chen et al., 2012).

Au niveau le plus élémentaire, les Big data contribuent permettent d'obtenir une meilleure vue d'ensemble du monde qui nous entoure. Les données relatives aux préférences des utilisateurs, à leurs communications et à leurs comportements en ligne peuvent être recueillies et traitées à travers des algorithmes spécialisés, afin d'identifier certains modèles de comportement ou des corrélations entre différents utilisateurs, qui seront ainsi classées dans certaines «catégories» en fonction de leurs comportements actuels, passés et futurs (Brown & al., 2011).

Ces pratiques se rencontrent surtout sur Internet, où le profilage des utilisateurs peut se faire à un rythme beaucoup plus rapide et à un niveau beaucoup plus granulaire. Tout activité en ligne est, de nos jours, transformée en données. La plupart des appareils avec qui les gens interagissent (qu'ils s'agissent d'ordinateurs, de tablettes, de téléphones ou de tous objets dotés de capteurs, tels que les nouveaux réfrigérateurs ou thermostats intelligents) collectent des données à propos de ces interactions: des données sur les individus eux-mêmes, des données sur leurs préférences, leurs goûts ou leurs besoins particuliers, des données sur leurs activités et leurs comportements, etc. Tout ce que les internautes disent ou font sur une plate-forme donnée laisse forcément une trace qui peut être suivie et / ou contrôlée par l'opérateur de la plate-forme. Aujourd'hui, il est fréquent que ces données soient collectées par les intermédiaires en ligne, et ensuite utilisées comme point d'entrée pour l'analyse des grandes masses de données, en vue de pouvoir mieux comprendre et pourquoi pas prévoir les comportements passés et futurs des internautes.

En effet, comme la quantité de données augmente constamment, l'effectivité et la fiabilité des analyses de Big data augmentent par conséquent. En agrégeant de grandes masses de données provenant de différentes sources, des outils d'analyse de plus en plus sophistiqués (comprenant l'extraction des données, la modélisation statistique, et l'apprentissage automatisé) peuvent être déployés non seulement pour déduire des informations sur les traits et les caractéristiques distinctives des utilisateurs individuels, mais aussi afin de prévoir leurs comportements futurs grâce à des analyses statistiques dites prédictives (Russom, 2011). Les Big data sont ainsi de plus en plus invoqués non seulement dans le but de mieux *comprendre* les individus, mais aussi dans le but de *prévoir* leurs activités, en estimant la probabilité pour différents types d'individus à se

comporter d'une manière ou d'une autre (Truve, 2011).
Par exemple, en se fondant sur des techniques de *data mining* avancées et des algorithmes de corrélation statistique, les compagnies de cartes de crédit peuvent identifier les clients qui ont une histoire d'amour, reconnaître ceux qui ont récemment emménagé dans une nouvelle habitation, ou même prévoir un divorce imminent (Duhigg, 2009). Plus généralement, en analysant les comportements distinctifs des internautes (y compris l'historique de recherche et de navigation, les périodes et la vitesse de navigation, etc.) il est possible de déterminer l'humeur et personnalité des utilisateurs, ainsi que leur état d'esprit, et même parfais d'identifier des signes spécifiques de dépression. Au-delà des applications évidentes liées au marketing et à la publicité cible, ces informations peuvent, bien sûr, également être utilisées pour le bénéfice des citoyens. En combinant les dossiers de santé d'un patient avec les données recueillies par les dispositifs portables ou des capteurs personnels, les services de soins de suivi peuvent identifier des troubles sous-jacents et protéger ainsi leurs patients de maladies imminentes (Barrett et al., 2013) —voir notamment les messages de Facebook, utilisés pour identifier des signes de dépression *post-partum* avec un niveau de précision relativement élevé (De Choudhury et al., 2013).
Aujourd'hui, certaines entreprises exploitent déjà les nouvelles possibilités offertes par les techniques de *data mining* et d'inférence statistiques afin de proposer des offres innovantes à leurs clients. Les compagnies d'assurance sont les pionnières dans la matière, elles se fondent sur l'analyse des grandes masses de données afin d'établir le montant des primes qui devraient être payées, sur une base individuelle, par chaque client. Les plus avancées à cet égard sont les compagnies d'assurance sanitaires, qui reposent sur des algorithmes de plus en plus sophistiqués afin de distinguer les bons clients —*i.e.* les individus en bonne santé— des mauvais clients—*i.e.* les individus qui sont malades ou susceptibles de le devenir (Groves et al., 2013). Il en est de même pour certaines compagnies d'assurance automobile -comme Progressive, Allstate ou Travellers Companies— qui suggèrent à leurs clients d'installer un dispositif de suivi spécialisé dans leurs voitures, de façon à collecter des données relatives à leurs habitudes de conduite (i.e. la vitesse, l'accélération, les freinages brusques, etc.) pendant une certain période de temps, et ajuster ensuite automatiquement la prime sur la base des données recueillies.

B. Vie privée: sur les responsabilités légales et morales des opérateurs en ligne de communiquer des informations personnelles à des tiers.

Pendant longtemps, l'utilisation des techniques de contrôle et de surveillance intrusives ont été justifiées sur la base de l'application de la loi. De plus en plus, aujourd'hui, les mêmes technologies sont utilisées conjointement avec des techniques de *data mining* et d'inférence statistique, en vue non seulement de préserver la sécurité nationale, mais aussi dans le but de construire une société plus réactive, interconnectée et personnalisée —où la personnalisation des services semble être devenue un *quid pro quo* d'une automatisation croissante fondée sur la surveillance, la réglementation et, bien sûr, la publicité ciblée. Ainsi, on s'éloigne progressivement de la notion traditionnelle de "surveillance de masse" vers une conception plus radicale, et potentiellement plus intrusive de "*total information awareness*" (Lee, 2013): la surveillance n'est plus considérée comme un coût nécessaire à payer pour assurer la sécurité

nationale, mais plutôt comme un atout, qui permet aux utilisateurs d'obtenir un service plus personnalisé et mieux adapté à leur besoins.

Étant donné l'accès exclusif des grands opérateurs en ligne à une grande quantité d'informations collectées et/ou crées par eux-mêmes (Han, 2013), il convient de se demander si ces opérateurs ont une l'obligation morale ou une responsabilité de communiquer les informations relatives à leur base d'utilisateurs à des parties tierces. L'article 8 de la Convention Européenne des Droits de l'Homme spécifie un certain nombre d'exceptions à la règle générale pour le respect de la vie privée, dès lors que cela serait nécessaire pour préserver la sécurité nationale, pour prévenir un crime ou un tort, et pour protéger l'ordre public et la santé des citoyens. Ainsi, les opérateurs en ligne sont-ils moralement obligés à divulguer des informations personnelles —au prix d'empiéter sur la vie privée des internautes— afin de promouvoir l'intérêt général?

Prenons l'exemple d'une opérateur de suivie de santé, qui aurait identifier que l'un de ces utilisateurs est à risque de rencontrer un diabète —cet opérateur a-t-il le droit de communiquer cette information, ainsi que les habitudes alimentaires de l'individu, à un docteur? De même, dans le cas d'un opérateur qui aurait identifié un utilisateur tombé en dépression et manifestant des comportements qui indiquerait que cet individu considère le suicide, est-ce que cet opérateur a le droit (ou le devoir) de protéger cet utilisateur en limitant la nature des contenus auquel il peut être exposé et/ou en communicant ces symptômes à une autorité sanitaire? D'après l'article 7 de la directive européenne sur la protection des données personnelles, il semblerait que, en effet, le traitement et l'utilisation des données personnelles peut être fait sans le consentement de la personne concernée dès lors que cela serait "nécessaire pour protéger les intérêts vitaux" de cette personne.

La question est plus critiques lorsque le *data mining* révèle une tendance de certains individus à se comporter de manière violente, ou une propension pour ces individus à s'engager dans des activités criminelles. Les autorités publiques utilisent déjà des outils de *data mining* avancés afin d'identifier et recueillir des preuves d'activités terroristes (Mena, 2003). Les caméras de surveillance sont toujours plus déployées avec des logiciels d'analyses destinés à détecter des modèles de comportements qui pourrait demander l'intervention des forces de police. Cela, combiné avec des outils d'analyse statistique, permet d'évaluer la probabilité qu'un crime soit commit dans une certain zone géographique (Chen & al., 2012). Ainsi, il s'agit de savoir si, dans le cas d'individus qui révèlent des tendances criminelles, leur identité devrait être immédiatement communiqué aux autorités publiques?

Suite aux révélations de Snowden, la collection, l'agrégation et le traitement massif des données relatives aux comportement et aux communications en ligne des individus, dans le but de profiler ces individus dans des catégories spécifiques selon le niveau de risque qu'ils présentent semble soulever plusieurs problématiques. En effet, alors que les pratiques de surveillance sont considérées (par certains) comme une activité légitime lorsqu'elles sont performées par des autorités publiques agissant dans le but de préserver l'ordre public, comment est-ce que cela se traduit dans le secteur privé ? Est-ce que des opérateurs tels que Google, Twitter ou Facebook ont le droit d'empiéter sur la vie privée des internautes en reportant des activités suspectes à la

police, ou en suggérant que certains utilisateurs qui révèlent des modèles de comportements criminels soient mis sous surveillance?

Dans la mesure où cela constituerait une violation des lois sur la protection des données personnelles dans de nombreux pays, il est difficile d'imaginer que de telles pratiques soient légitimes. D'ailleurs, indépendamment de la légitimité de ces divulgations, la valeur juridique des informations issues des analyses statistiques peut être remise en question. À cet égard, l'article 15 de la directive sur la protection des données personnelles spécifie que, alors que le résultats des analyse de Big data peuvent être considérés au sein d'un procès, toute information résultant des techniques de *data mining* ou de profilage automatisé ne peuvent pas constituer la *seule base* pour une décision juridique.[9]

Enfin, l'utilisation d'outils d'analyse descriptive ou statistique afin de faciliter l'application des lois n'est pas omise de certains coûts. Bien que cet utilisation puisse contribuer à assurer de l'ordre en société, et pourrait éventuellement mené à une société plus sûre et contrôlée, il y a, cependant, des risques importants liés au fait de donner aux opérateurs en ligne le droit (ou même l'obligation) de divulguer des informations personnelles à certaines autorités publiques ou privées, dans la mesure où ces informations sont issues d'analyses statistiques et d'inférence. En effet, les techniques d'analyses prédictives ne peuvent pas prévoir le future, elles peuvent uniquement estimer la probabilité qu'un événement donné se produise. Ainsi, étant donné le bias inhérent dans la collecte et le traitement des données collectées, agir sur la base de prédictions risque effectivement de détourner la réalité au bénéfice (ou au détriment) de certaines catégories d'acteurs.

C. Au-delà de la vie privée: manipulation des données et déterminisme algorithmique

En plus des problématiques évidentes soulevées par les Big data en ce qui concerne le droit au respect de la vie privée, les analyse descriptives, prédictives et d'inférence statistiques peuvent aussi contribuer (aussi bien directement que indirectement) de manière significative à influencer les comportements présents et futurs des utilisateurs, en modifiant leurs perceptions, leur états d'âme, et potentiellement aussi leurs actions.

La notion de "*filter bubble*" proposée par Eli Pariser (2011) illustre parfaitement la manière dont nous sommes tous entourés par des algorithmes dont le but est, en fin de compte, de filtrer les informations auxquelles nous sommes exposés. Ces algorithmes sont d'autant plus précieux en vue de la quantité croissante d'information qui nous entoure aujourd'hui. Or, dans la mesure où différents individus reflètent des intérêts, des préférences ou des besoins différents, afin d'être efficaces, ces algorithmes ont besoin d'apprendre à propos des personnes avec lesquelles ils interagissent, de manière à leur fournir l'information qui leur est la plus appropriée (c'est à dire, l'information la plus pertinente, la moins nocive, etc.). Évidemment, le seul moyen pour ces algorithmes de se renseigner sur les caractéristiques distinctives des utilisateurs avec qui ils

[9] Voir l'article 15 de la directive sur la protection des données personnelles, stipulant que "les États membres accordent le droit à toute personne de ne pas être soumise à une décision produisant des effets juridiques à son égard si cette décision est fondée uniquement sur le traitement de données automatisé destiné à évaluer certaines caractéristiques personnelles, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc. "

interagissent est à travers la collecte et le traitement des données collectées ou inférées à leur sujet. Par conséquent, le plus grand est le nombre de données disponibles, le plus précis ces algorithmes pourront être. Outre à traiter les données, les algorithmes sont aussi responsables de l'extraction et de la production d'information, de la création de profils d'utilisateurs qui s'affinent constamment au fil du temps, dès lors que les algorithmes ont accès à de nouvelles données. Selon la catégorie où ils ont été classées, des utilisateurs différents seront exposés à différentes typologies de services et d'informations –ce qui pourraient affecter de manière significative aussi bien leur autonomie que leur liberté d'action (Pazzani & Billsus, 2007).

Par exemple, l'année dernière, l'équipe scientifique de Facebook a entrepris une étude pour mesurer la "contagiosité" des émotions en ajustant la positivité ou la négativité du flux de nouvelles (NewsFeed)[10] auquel les utilisateurs de Facebook sont exposés (Kramer et al., 2014). Alors que Facebook a mené ce genre d'expériences pour de nombreuses années (Bakshy & al., 2014), cette dernière a été perçu comme étant problématique en raison des implications éthiques qui en découlent. Tout d'abord, il est incertain si l'expérience a été faite conformément à la doctrine du consentement éclairé. En effet, nonobstant le fait que, en acceptant les conditions d'utilisation de Facebook, les utilisateurs doivent consentir à ce que Facebook utilise leurs données pour des "*opérations internes, y compris le dépannage, l'analyse de données, la recherche et l'amélioration du service*," Facebook n'avait pas informé correctement les utilisateurs à propos du type de recherche auxquels ils pourraient être soumis, éliminant ainsi la possibilité pour les individus de faire objection à l'étude. En outre, l'étude elle-même pose série de questions éthiques, puisque Facebook manipulait les états émotionnels des utilisateurs d'une façon qui ne pouvait pas être prévue par les utilisateurs, et sans fournir aucune information sur si les principes éthiques ont été effectivement suivis au cours du processus. En ce sens, il n'y avait pas de "consentement éclairé", car les utilisateurs étaient incapables de délimiter la différence entre les conditions naturelles et expérimentales.

Évidemment, indépendamment de cette expérience, le NewsFeed de Facebook est déjà fortement manipulée par des algorithmiques de recommandations —le flux de nouvelles dans son état pur est seulement affiché aux utilisateurs qui le demandent expressément. L'algorithme de Facebook manipule le NewsFeed (par exemple, en favorisant les messages qui contiennent des images, ou ceux qui citant certaines marques) dans le but de servir les intérêts (commerciaux) de Facebook. La manipulation est bien sûr aussi réalisée pour retenir les utilisateurs dans le système, en leur fournissant les contenus que Facebook *pense* être les plus adaptés à leurs profiles, et qui sont donc susceptible de les inciter à revenir. À cet égard, changer les contenus qui sont affichés dans le NewsFeed est utile pour mesurer l'efficacité de l'algorithme (en vue d'améliorer la rétention des utilisateurs). Mais de nombreuses autres raisons (moins évidentes) peuvent également contribuer à façonner l'algorithme. Avec cette expérimentation, Facebook a tenté d'influencer la perception de ce qu'est la «réalité» pour ces utilisateurs, afin d'affecter leur humeur ou même

[10] Plus précisément, Facebook a manipulé le contenu proposé à plus de 600.000 utilisateurs afin de déterminer si cela pourrait affecter leur état émotionnel. Ces résultats indiquent que les émotions exprimées par les utilisateurs de Facebook influencent les émotions des autres utilisateurs. Cela constitue une preuve de contagion massive à l'échelle des réseaux sociaux. Pour plus de détails, voir Kramer & al. (2014)

leurs actions. Déjà en 2010, Facebook avait mené une étude concernant la participation des électeurs, dans le but d'analyser si en communiquant à ces utilisateurs que leurs amis avaient voté les aurait "pousser" à se rendre à voter —une expérience qui aurait soi-disant mobilisé plus de 60.000 électeurs.[11] Des expériences de ce type se produisent quotidiennement, la plupart du temps à des fins de marketing —voir notamment les "histoires sponsorisés" de Facebook, qui utilisant les messages des utilisateurs pour publiciser des produits à leurs amis.

Alors que la manipulation des contenus n'est un mal en soi, en effet presque toutes les sources de contenus aujourd'hui sont manipulées,[12] elle doit se faire d'une manière qui ne va pas contre les intérêts des utilisateurs. Même s'ils ont obtenu le consentement de la part des utilisateurs pour le traitement des données à caractère personnel, les fournisseurs de services en ligne doivent être tenus responsables des conséquences qui découlent de la manipulation de l'expérience des utilisateurs, surtout lorsque cela implique l'analyse des traits distinctifs et caractéristiques d'un ensemble particulier d'utilisateurs, de manière à influer leurs idées ou leurs comportements. Cela est lié au concept éthique de *bénéficience*, qui exige que toutes les pratiques aux fins de recherche soient conçues pour ne cause nuisance aux sujets de la recherche (Pellegrino, 1988). En d'autres termes, toute expérience doit être entreprise de manière telle à éviter que des individus résultent négativement affecté par celle-ci, et —si l'expérience comporte des risques— à atténuer le dommage qui pourrait être encouru par les personnes concernées.

Or, dans le cas de Facebook, lors de son expérimentation visant à manipuler unilatéralement le NewsFeed de ses utilisateurs (et modifiant ainsi les contenus auxquels ils ont été exposés), aucun mécanisme n'avait été mis en place pour les protéger contre tout possible impact négatif que la recherche pourrait causer. L'expérience a été réalisée dans les coulisses, sans aucun système de garanties visant à limiter les malaises potentiels qui pourraient résulter de cette manipulation émotionnelle. À cet égard, la suggestion de Jonathan Zittrain de traiter tout prestataire de services chargé du traitement de données personnelles et d'autres informations sensibles comme un "fiducaire informationnel" pourrait être un bon point de départ. Selon Zittrain, le degré de confiance que les individus donnent à de nombreux opérateurs en ligne est de nature telle à donner lieu à un devoir supplémentaire qui les obligerait à agir selon certains principes de "fiduciarisation" —de même que les avocats et les médecins ne sont pas autorisés à utiliser des informations sensibles de leurs clients pour un usage autre que celui pour lequel elles avaient été

[11] Globalement, les utilisateurs notifiés du vote de leurs "amis" étaient pour 0.39% plus susceptibles de se rendre à voter que ceux du groupe de contrôle —et la décision de se rendre à voter a également eu des répercussions sur le comportement des amis proches de Facebook, même si ces derniers n'avaient pas reçu le message d'origine. Les chercheurs ont conclu que, suite à cette expérimentation, Facebook a directement mobilisé 60.000 électeurs, et, grâce à l'effet d'entraînement, a causé 340.000 votes supplémentaires ce jour-là. Pour plus de détails, voir Zittrain, J. (2014).

[12] Par exemple, les institutions financières, comme les banques, comptent souvent sur l'analyse prédictive pour déterminer la fiabilité de leurs clients et réduire la probabilité d'avoir des clients défaillants sur leurs paiements. Les supermarchés (qui bénéficient de fort contacts avec la clientèle) effectuent aussi de nombreuses expérimentations à travers leurs points de vente en ligne et hors ligne, afin de créer de meilleures relations de consommation et des programmes de fidélité. Les opérateurs de téléphonie mobile et les industries du divertissement expérimentent aussi avec l'analyse des grandes masses de données (par exemple en reliant les informations client avec leurs comportements réels) afin de cibler plus efficacement les consommateurs. Voir McKinsey (2011).

initialement divulguée (Zittrain, 2014).
Dans son ensemble, l'étude de Facebook constitue une illustration claire de la façon dont l'analyse des grandes masses de données —même si réalisés avec le consentement explicite des personnes concernées— pourrait être employé pour des raisons qui vont effectivement contre les intérêts des utilisateurs. L'expérience a reçu beaucoup d'attention dans les médias et a crée un débat considérable autour des responsabilités légales et morales des intermédiaires en ligne dès lors qu'ils ne se limitent pas seulement à collecter et à traiter des informations, mais aussi à agir selon les résultats issus de leur traitement.

D. Limites à l'autonomie individuelle: lorsque les prédictions se transforment en actions

L'analyse de grandes masses de données fournit de précieuses indications concernant l'état actuel des choses, ainsi que la probabilité de développements futurs —permettant ainsi une prise de décisions plus éclairée. Mais que se passe-t-il lorsque de simples prédictions se transforment en actions? Que faire lorsque le résultat des analyses descriptives et / ou prédictives sont invoquées afin d'établir un plan d'action spécifique qui va encourager ou décourager certaines pratiques?
Indépendamment de si les informations personnelles peuvent être communiquées de façon légitime aux autorités publiques, la question reste de savoir si les opérateurs en ligne ont le droit (ou le devoir) d'agir sur les données qu'ils ont recueillies, déduites ou inférées? Bien que la divulgation d'information à caractère personnel pourrait être limitée, ou pour le moins régulée par les règles portant sur la protection des données personnelles, est-ce que les opérateurs en ligne peuvent (ou doivent) intervenir sur la base d'analyses et de prédictions, contraignant les activités de certaines catégories d'utilisateurs classifié comme une menace potentielle, afin de réduire le potentiel pour que des activités nuisibles ou indésirables se produisent?
Un des aspects les plus critiques de l'analyse des grandes masses de données est lié à la possibilité de faire appliquer la loi de manière prescriptive (*a priori*). En effet, dans un contexte caractérisé par la collecte généralisée des données, la surveillance de masse et la manipulation algorithmique, l'utilisation des Big data en combinaison avec les techniques d'inférence statistique est devenu une question très controversée. Alors que ces pratiques pourraient, en effet, diminuer le risque d'activités criminelles ou illégitimes, le fait d'agir sur des analyses statistiques afin de prévenir certaines activités sur la simple base d'inférences ou de prédictions pourrait conduire à des limitations injustes sur les libertés fondamentales des individus.
Le problème n'est pas lié directement au concept de *vie privée*, plutôt qu'à celui d'*autonomie*: un concept qui englobe plusieurs domaines de la vie humaine, de la liberté d'expression à la liberté d'accès à l'information, de la gouvernance des communautés à l'autonomie individuelle. Les règles sur la protection des données personnelles ne sont actuellement concernées que par la collecte, l'agrégation et le traitement des données personnelles, qui ne peut se faire sans le consentement des personnes concernées. Or, la loi ne réglemente pas la manière dont ces données peuvent être légitimement exploitées par le contrôleur des données agissant dans les limites de son mandat. En d'autres termes, tant que les lois sur la protection des données personnelles ne sont pas violées, les utilisateurs ne peuvent pas faire recours contre les

opérateurs en ligne qui sont imposent effectivement des limites sur leur liberté d'agir.

Comme il a été vu précédemment, alors que les opérateurs en ligne ne sont pas (encore) en capacité d'agir afin de contrôler les comportements de certains individus en fonction de leurs comportements passés, ils sont peuvent cependant limiter leur capacité de choisir librement les informations auxquelles ils veulent être exposés. Mais les filtrage des contenus auxquels les utilisateurs peuvent accéder n'est qu'une partie du problème. Un autre problème —peut-être plus important— est que la plupart de ces algorithmes ne se limitent pas à filtrer les contenu, ils réagissent aussi aux résultats fournis par l'analyse des grandes masses données, en personnalisant leur offre pour mieux s'adapter aux profils des utilisateurs —limitant ainsi la portée des actions que les utilisateurs peuvent effectuer par des moyens techniques.

En effet, bien qu'il est vrai que, dans le cyberespace, "*le code c'est la loi"* (Lessig, 1999), aujourd'hui plus que jamais, la régulation des comportements en ligne est réalisé au moyen de la régulation algorithmique, où ce sont les données qui contrôlent effectivement le code en question (Mayer-Schönberger et Cukier, 2013). Ce que les utilisateurs peuvent ou ne peuvent pas faire sur Internet est, en effet, dicté par le code source de plates-formes et des protocoles qui régissent le réseau. Mais les utilisateurs sont de plus en plus dépendants des algorithmes qui sous-tendent ces plates-formes, qui vont en fin de compte déterminer comment ces plates-formes interagissent avec leur environnement.

Par conséquent, les résultats issus d'un algorithme (qu'ils soient bons ou mauvais) pourrait avoir un impact considérable sur le la vie des individus. D'une part, ceux qui ont été injustement profilés comme quelque chose qu'ils ne sont pas (par ex. les amateurs de jazz, les militants d'extrême-droite, ou les homosexuels) pourraient éventuellement le devenir (par ex. les personnes exposées à beaucoup de jazz pourraient progressivement développer un goût pour le jazz, les personnes exposées à des contenu d'extrême droite pourrait finir par assimiler ces points de vue, etc.) ou tout simplement être traitées comme si elles l'étaient (par ex. les personnes qui ont été profilées comme homosexuels pourrait être victime de discrimination, indépendamment de leur préférences réelles). D'autre part, les individus considérés comme une menace potentielle pour la société (à cause de quelque chose qu'ils ont fait, dit, ou peut-être implicitement exprimés) pourraient être soumis à un régime plus contrôlé, laissés avec seulement une série limitée d'actions qu'ils peut effectuer librement sur la plate-forme.

Quelque chose qui ressemblait fortement à de la science-fiction il y a quelques années (voir par exemple l'ouvrage de George Orwell *Mil Neuf Cent Quatre-vingt-quatre,* celui de Philip K. Dick *Minority Report,* ou même *Gattaca* d'Andrew Niccol) est maintenant de plus en plus proche de la réalité. S'il suffit de refléter certains comportements afin de devenir un suspect, la présomption d'innocence pourrait être mis en question (Kerr et Earle, 2013) alors que de plus en plus d'utilisateurs sont *présumés coupables avant d'être prouvés innocents.*

Le problème fondamental de la gouvernance algorithmique est essentiellement de deux ordres. Tout d'abord, étant donné que les opérations de nombreuses plates-formes en ligne reposent sur des algorithmes de *data mining* sophistiqués qui sont nourris avec des données fournies explicitement ou implicitement par les utilisateurs —ainsi que les informations qui ont été

extraites, dérivés ou déduites par les algorithmes sur lesquels ces logiciel tournent— la seule façon pour les utilisateurs de comprendre le fonctionnement de ces plates-formes est connaître l'ensemble des données qui sont fournies à ces algorithmes. Les opérateurs en ligne ont donc une responsabilité croissante face à leurs utilisateurs de communiquer non seulement les logiques internes et les opérations des algorithmes qu'ils utilisent, mais aussi les informations qu'ils ont recueillit (ou déduit) à propos de leur base d'utilisateurs (que ces informations qualifient ou pas comme des données personnelles). Deuxièmement, étant donné que ces algorithmes sont susceptibles d'évoluer au fil du temps à mesure qu'ils apprennent des nouvelles choses de leur environnement, il est extrêmement difficile pour quiconque —y compris les développeurs— d'examiner les différentes composantes et les opérations des algorithmes sous-jacents, afin de déterminer si un acte répréhensible s'est effectivement produit. En outre, dans la mesure où l'analyse des données peut avoir un effet préventif sur les actions des individus, il est impossible de juger de l'exactitude et / ou la fiabilité de ces algorithmes, car ils modifient de façon irréversible la réalité d'une manière à rendre impossible l'évaluation *a posteriori* de ce qui se serait ont passé autrement, si les algorithmes n'aurait pas été exécutés.

Conclusion

À l'ère de l'informatique en nuage, où presque toute activité en ligne peut être observée par les fournisseurs de services (Stein, 2011), il est important de reconnaître que les avantages des Big data doivent être contrebalancés avec les risques que les opérateurs en ligne collectent, déduisent ou infèrent un nombre excessif d'informations (Bollier et Firestone, 2010). D'une part, l'agrégation de données provenant de nombreuses sources différentes permet aux fournisseurs de services de profiler leurs utilisateurs en catégories significatives, afin de leur fournir un service plus personnalisé dans la mesure où il est plus adapté à leurs préférences et goûts individuels (Brown et al., 2011). D'autre part, cependant, les outils de *data mining* et d'inférence statistique pourraient empiéter sur les droits fondamentaux des utilisateurs tels que le droit à la vie privée, la liberté d'expression ou le droit d'accès à l'information. Avec la collecte généralisée de données (ou la surveillance de masse), il est possible pour les opérateurs en ligne d'acquérir des connaissances approfondies sur leur base d'utilisateurs, afin de mieux comprendre leurs intérêts ou leurs besoins actuels, mais —potentiellement— aussi de prévoir leurs actions ou comportements à venir (McAfee & Brynjolfsson, 2012).

En plus des menaces évidentes à la vie privée que cela pourrait entraîner, ces pratiques sont également susceptibles de limiter l'autonomie des individus. En effet, dans la mesure où l'information résultante de ces analyses de données peut effectivement être utilisée comme base pour caractériser les services offerts aux utilisateurs, les opérateurs en ligne ont la capacité d'influencer sensiblement l'autonomie des individus. L'expérience de Facebook est seulement un exemple de comment la collecte généralisée de données, combinée avec les techniques de *data minin*g et d'inférence statistiques, permet à de grandes ligne opérateurs d'influencer les utilisateurs sur plusieurs dimensions de leur vie —en commençant par influencer leurs états

d'âmes et leurs émotions, pour finir par l'altération de leurs actions et la modification de leurs comportements. En fin de compte, le danger est que —suite à l'automatisation croissante et la gouvernance algorithmique qui caractérise le monde numérique, l'analyse des grande masses de données puissent fournir des résultats qui ne peuvent plus être considérées comme une représentation adéquate de la réalité, mais plutôt comme un véritable outil capable de transformer les prédictions en réalité.

Avec la monté en popularité de la surveillance généralisée, il devient crucial pour les utilisateurs de reconnaître les implications de la gouvernance algorithmique proposée par les fournisseurs de services en ligne. Le problème, ce n'est pas que *"la vie privée en ligne est morte"*[13], mais plutôt qu'il est de plus en plus difficile de protéger les libertés individuelles. Les utilisateurs doivent se rendre compte que chaque décision déléguée à un algorithme constitue une menace non seulement pour leur droit à la vie privée, mais aussi à leur autonomie individuelle.

Si les utilisateurs ont désormais besoin de renoncer à leur vie privée afin de bénéficier d'un service plus personnalisé, ou s'ils doivent donner leur consentement à ce que leurs données personnelles soient collectées, regroupées et traitées au sein de grands jeux de données afin de bénéficier des services d'une plate-forme en ligne, le droit au respect de la vie privée —bien que toujours applicable en théorie— devient pratiquement inconséquent. D'ailleurs, si les résultats des analyses descriptives ou prédictives sont utilisées, internement au sein d'une organisation, comme un outil pour déterminer les contenus auxquels les utilisateurs seront exposées, comme un moyen pour encourager (ou décourager) certains types de comportements; ou même comme un moyen pour limiter la liberté d'action des individus, il devient évident que le droit à la vie privée à lui seul ne peut pas être sollicité pour assurer l'autonomie individuelle.

Le temps est venu de commencer à penser au-delà du concept de «vie privée». Des motifs juridiques alternatifs doivent être identifiés afin de préserver la possibilité pour les utilisateurs d'agir de leur propre volonté, indépendamment du fait qu'ils aient renoncé ou pas à leurs droits au respect de la vie privée. Seulement ainsi pourrons-nous cesser d'agir comme de simples «utilisateurs» ou «consommateurs» de services en ligne, pour devenir alors de vrais "citoyens" désireux de préserver nos droits et nos libertés fondamentales dans le monde numérique.

Références

Arthur, L. (2013). *Big Data Marketing: Engage Your Customers More Effectively and Drive Value*. John Wiley & Sons.

Bakshy, E., Eckles, D., & Bernstein, MS (2014, April). Designing and deploying online field experiments. In *Proceedings of the 23rd international conference on World wide web* (pp. 283-292). International World Wide Web Conferences Steering Committee.

Barrett, MA, Humblet, O., Hiatt, RA, & Adler, NE (2013). Big Data and Disease Prevention: From Quantified Self to Quantified Communities. *Big Data*, *1*(3), 168-175

Berry, MJ, & Linoff, GS (2004). *Data mining techniques: for marketing, sales, and customer relationship*

[13] Revendiqué par Mark Zuckerberg, fondateur de Facebook, à la cérémonie de Crunchie 2010 à San Francisco.

management. Wiley. com.
Bollier, D., & Firestone, CM (2010). *The promise and peril of big data* (p. 56). Washington, DC, USA: Aspen Institute, Communications and Society Program
Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, *15*(5), 662-679.
Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services. *International Journal of Law and Information Technology*, *19*(3), 187-223.
Brown, B., Chui, M., & Manyika, J. (2011). Are you ready for the era of 'big data'?. *McKinsey Quarterly*, *4*, 24-35.
Bughin, J., Livingston, J., & Marwaha, S. (2011). Seizing the potential of 'big data'. *McKinsey Quarterly*, 103-109.
Bus, J., & Nguyen, MHC (2013). Personal Data Management–A Structured Discussion. *Digital Enlightenment Yearbook 2013: The Value of Personal Data*, 270.
Cavoukian, A., & Jonas, J. (2012). Privacy by design in the age of big data.*Office of the Information and Privacy Commissioner*.
Cambria, E., Rajagopal, D., Olsher, D., & Das, D. (2013). Big social data analysis. *Big Data Computing*, 401-414.
Chen, H., Chiang, RH, & Storey, VC (2012). Business Intelligence and Analytics: From Big Data to Big Impact. MIS quarterly, 36(4), 1165-1188
Cukier, K., & Mayer-Schoenberger, V. (2013). Rise of Big Data: How it's Changing the Way We Think about the World, The. *Foreign Aff.*, *92*, 28.
Cumbley, R., & Church, P. (2013). Is "Big Data" creepy?. *Computer Law & Security Review*, *29*(5), 601-609.
Craig, T., & Ludloff, ME (2011). *Privacy and big data*. O'Reilly Media, Inc.
Davies, T. (2010). *Open data, democracy and public sector reform: A look at open government data use from data. gov. uk*. Practical Participation.
De Choudhury, M., Counts, S., & Horvitz, E. (2013, April). Predicting postpartum changes in emotion and behavior via social media. In *Proceedings of the SIGCHI Conference on Human Factors in Computing* Systems (pp. 3267-3276). ACM
Duhigg, C. (2009). What does your credit-card company know about you. New York Times, 12
ENISA (2012). The right to be forgotten, between expectations and practice. Report of the European Network and Information Security Agency
Espinosa, JA, & Money, W. (2013, January). Big Data: Issues and Challenges Moving Forward. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 995-1004). IEEE.
Franks, B. (2012). *Taming the big data tidal wave: Finding opportunities in huge data streams with advanced analytics (Vol. 56). Wiley. com.*
Golle, P. (2006). Revisiting the uniqueness of simple demographics in the US population. In Proceedings of the 5th ACM workshop on Privacy in electronic society (pp. 77-80). ACM.
Groves, P., Kayyali, B., Knott, D., & Van Kuiken, S. (2013). The 'big data'revolution in healthcare. McKinsey Quarterly.
Han, J. (2013). The ethics of big data. Living Ethics: Newsletter of the St. James Ethics Centre, (92), 7.
International Data Corp. (2012), Worldwide Big Data Technology and Services 2012-2015 Forecast. IDC, March 7, 2012.

Joseph, RC, & Johnson, NA (2013). Big Data and Transformational Government. IT Professional, 15(6), 43-48.
Kaisler, S., Armour, F., Kerr, I., & Earle, J. (2013). Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy. Stanford Law Review Online, 66, 65.
Koops, BJ (2011). Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice. SCRIPTed, Vol. 8, No. 3, pp. 229-256, 2011;
Kramer, AD, Guillory, JE, & Hancock, JT (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, 201320040.
Laney, D. (2012). The Importance of'Big Data': A Definition. *Gartner, Inc*.
LaValle, S., Lesser, E., Shockley, R., Hopkins, MS, & Kruschwitz, N. (2011). Big data, analytics and the path from insights to value. *MIT Sloan Management Review*, *52*(2), 21-31.
Lazar, N. (2012). The Big Picture: Big Data Hits the Big Time. *CHANCE*, *25*(3), 47-49.
Lee, N. (2013). Total Information Awareness. In *Facebook Nation* (pp. 169-195). Springer New York.
Lessig, L. (1999). *Code: And other laws of cyberspace*. Basic Books (AZ).
Lohr, S. (2012). The age of big data. *New York Times*, *11*.
Lops, P., de Gemmis, M., & Semeraro, G. (2011). Content-based recommender systems: State of the art and trends. In Recommender Systems Handbook (pp. 73-105). Springer US.
Mancini, F., & O'Reilly, M. (2013). New technology and the prevention of violence and conflict. Stability: International Journal of Security and Development, 2(3), Art-55.
Manovich, L. (2011). Trending: the promises and the challenges of big social data.
Mantelero, A. (2013). "The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'". Computer Law & Security Review29 (3): 229–235. doi:10.1016/j.clsr.2013.03.010.
Mayer-Schönberger, V., & Cukier, K. (2013). Big Data: A Revolution That Will Transform How We Live. *Work and Think. London: John Murray*
McAfee, A., & Brynjolfsson, E. (2012). Big data: the management revolution.Harvard business review, 90(10), 60-66.
McKinsey (2011). Big data: The next frontier for innovation, competition, and productivity. McKinsey Global Institute. June 2011.
Mena, J. (2003). Investigative data mining for security and criminal detection. Butterworth-Heinemann
Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin UK.
Pazzani, MJ, & Billsus, D. (2007). Content-based recommendation systems. In The adaptive web (pp. 325-341). Springer Berlin Heidelberg.
Pellegrino, ED (1988). For the patient's good: The restoration of beneficence in health care.
Richards, NM, & King, JH (2013). Three Paradoxes of Big Data. Stanford Law Review Online, 66, 41.
Rosen, J. (2012). The right to be forgotten. Stanford law review online, 64, 88.
Russom, P. (2011). Big data analytics. TDWI Best Practices Report, Fourth Quarter.
Simanis, E., & Hart, S. (2012). Innovation from the inside out. Image.
Stein, J. (2011). Data mining: How companies now know everything about you.Time Magazine.
Stephens, M. (2014). Only the powerful will benefit from'the right to be forgotten'. The Guardian, May, 18.
Swan, M. (2012). Sensor mania! The Internet of Things, wearable computing, objective metrics, and the Quantified Self 2.0. Journal of Sensor and Actuator Networks, 1(3), 217-253.
Swan, M. (2013). The Quantified Self: Fundamental Disruption in Big Data Science and Biological

Discovery. Big Data, 1(2), 85-99.
Oboler, A., Welsh, K., & Cruz, L. (2012). The danger of big data: Social media as computational social science. First Monday, 17(7).
Thompson, D. (2012). " I Agreed to What?": A Call for Enforcement of Clarity in the Presentation of Privacy Policies. Hastings Comm. & Ent. LJ, 35, 199-223.
Truvé, S. (2011). Big Data for the future: Unlocking the predictive power of the Web. Recorded Future, Cambridge, MA, Tech. Rep.
Witten, IH, & Frank, E. (2005). Data Mining: Practical machine learning tools and techniques. Morgan Kaufmann
Weber, RH (2011). The right to be forgotten: more than a Pandora's box?.Journal of intellectual property, information technology and e-commerce law, 2, 120-130
Wolf, G. (2010). The data-driven life. The New York Times, 28.
Zittrain, J. (2014). Facebook Could Decide an Election Without Anyone Ever Finding Out. New Republic.