Des données et des Hommes. Droits et libertés fondamentaux dans un monde de données massives.

Rouvroy, Antoinette

Publication date:
2016

Document Version
le PDF de l'éditeur

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, le 11 janvier 2016 T-PD-BUR(2015)09REV

BUREAU DU COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL [STE n° 108]

(T-PD-BUR)

« DES DONNEES ET DES HOMMES »
DROITS ET LIBERTES FONDAMENTAUX DANS UN MONDE DE DONNEES MASSIVES

Antoinette Rouvroy*

Les vues exprimées dans cet article relèvent de la responsabilité de l'auteur et ne reflètent pas nécessairement la position officielle du Conseil de l'Europe.

Direction Générale Droits de l'Homme et Etat de droit

* Permanent, Chercheuse qualifiée du FNRS au centre de Recherche en Information, droit et Société (CRIDS), Université de Namur, Belgique. Pour sa relecture attentive et les commentaires judicieux dont ce travail porte les marques, mes plus sincères remerciements vont à **Jean-Noël Colin**, Professeur en Faculté d'Informatique à l'Université de Namur. Mes remerciements vont également à **Alessandro Manteloro** pour ses suggestions extrêmement pertinentes à propos de certains éléments de la seconde partie de ce rapport.

Table des matières

AVERTISSEMENT

Afin de mieux cerner la nouveauté des traitements de type *Big Data* par rapport aux traitements de données à caractère personnel concernés notamment par la Convention 108 du Conseil de l'Europe, une première partie de notre rapport sera consacrée à la description conjointe des *données* concernées par le Big Data, des *processus de traitement* de ces données, et de certains *enjeux éthiques, juridiques et politiques* y afférents.

Le choix de traiter ensemble les aspects techniques et sociétaux résulte du constat d'une interdépendance inextricable entre les enjeux sémiotiques, épistémiques, éthique et politique dans le contexte des Big Data. Nous verrons par exemple que les pratiques statistiques impliquées dans les analyses de type Big Data instaurent une nouvelle manière de sous-traiter à des systèmes automatiques la tâche de faire surgir de la réalité numérisée elle-même, plutôt que de les instituer politiquement ou d'en convenir contractuellement, les catégories (de mérite, de besoin, de désirabilité,) présidant à la répartition des ressources et opportunités dans notre société.

Comprendre la rationalité des processus algorithmiques (datamining, machine learning,…) est donc un présupposé nécessaire à toute réflexion normative à propos des Big Data en termes d'Etat de droit et de droits et libertés fondamentaux. Il nous importera de tenir compte de l'évolution et de la diversité des processus de calcul impliqués dans les traitements de type Big Data.[1]

Les applications des nouvelles techniques d'analyse et d'exploitations des Big Data sont innombrables. La "classe" d'applications qui nous intéressera ici sera celui celle qui fait intervenir la modélisation des prédispositions et des comportements humains à des fins diverses sur base des données émanant des individus, des contextes dans lesquels ils vivent, ou produites automatiquement.[2]

[1] Il conviendrait notamment d'identifier le plus précisément possible les processus relevant du Data Mining, du Machine Learning, des Social Network Analysis, des Predictive Analytics, du "Sensemaking", du Natural Language Processing, de la Visualization,… dans la mesure où ces processus posent des enjeux spécifiques. Dans le présent rapport, cependant, nous nous sommes surtout intéressés au Data Mining et au Machine Learning tout en gardant à l'esprit que d'autres processus de traitements de type Big Data ont des implications marginalement spécifiques en termes de protection des données et de protection de la vie privée.

[2] Note intempestive: Nous aurions pu tout aussi bien ne plus distinguer entre l'humain et le non-humain dès lors que les Big Data n'ont pas, pour "unités", les individus, ni même les objets, mais les données - les notions d'individu, de sujet, de personne, ou même de groupe, de collectif, de communauté, sont, par définition pourrait-on dire, dissoutes et exclues de l'univers des Big Data - et dès lors que le phénomène des Big Data et des nouvelles méthodes de corrélation des données clôturent le réel numérisé sur lui-même, laissant de la sorte « à l'extérieur » les corps, les objets physiques, toute « chose » ayant une « forme » résiliente. Ce n'est pas par effet d'anthropocentrisme que l'on s'intéresse plus particulièrement à la modélisation des prédispositions et comportements humains, plutôt qu'à la modélisation des autres événements possibles du monde, mais parce que, d'avantage sans doute que les autres vivants et que les choses inanimées certainement, les humains réagissent généralement, et parfois de manière anticipative, aux descriptions et inscriptions dont ils font l'objet pour s'y conformer ou pour s'en écarter, et parce qu'ayant la faculté de parler, ils ont cette capacité de récalcitrance, de réplique, d'excédance à toute « nomination », à toute caractérisation ou profilage - dont ils font l'objet : les êtres humains « répondent » au nom d'homme, alors que les autres animaux sont privés de toute possibilité de réponse lorsqu'on les nomme, lorsqu'on les désigne unilatéralement(voir à cet égard Jacques Derrida, « L'animal que donc je suis », in. *L'animal autobiographique. Autour de Jacques Derrida*, Galilée, 1999, p. 283), même s'il n'est pas absolument exclu, quoi que douteux, qu'à l'inverse ils nous affublent d'un nom, entre eux,

Notre rapport se compose de deux parties. La première partie (**Les Big Data : enjeux techniques, épistémiques et sociétaux**) est une tentative d'identification de *ce qui fait la nouveauté radicale* du monde des *Big Data* et des enjeux sociétaux y afférents.

La seconde partie (**La Convention 108 du Conseil de l'Europe à l'ère des Big Data**) s'attèle, conformément au mandat confié, à détecter les possibilités de contribution du régime de protection des données à caractère personnel à la résolution de tout ou partie de ces enjeux sociétaux et à proposer quelques pistes de réflexion quant à l'évolution éventuelle de la Convention en vue de tenir compte du phénomène des Big Data. Vu la complexité des enjeux, induisant aussi une complexité dans leur dévoilement et leur exposition (il eût fallu pouvoir écrire en trois dimensions au moins), nous avons opté pour quelques solutions de présentation vouées à faciliter la lecture. Afin de les distinguer des autres considérations, les propositions concrètes que nous avons pu dégager sont présentées dans des encadrés. Chaque fois que nous faisons référence, sans plus de précision mais en caractères gras à des articles numérotés, il faut entendre que nous nous référons aux articles de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans la version amendée résultant des travaux du Comité consultatif de la Convention 108.[3]

Dans la mesure où le phénomène des données massives a vocation à concerner la quasi-totalité des secteurs d'activité et de gouvernement, il nous sera bien entendu impossible d'en dresser une liste exhaustive des enjeux actuels et futurs. Tout au plus pourrons – nous fournir quelques exemples dans lesquels se profilent des enjeux pertinents sous l'angle de la protection des données et, plus généralement, de la protection des droits et libertés fondamentaux.

1. LES *BIG DATA* : DESCRIPTION, ENJEUX TECHNIQUES, EPISTEMIQUES ET SOCIETAUX

1.1. Volume

L'univers numérique se composerait aujourd'hui de plus de mille-deux-cent milliards de milliards d'octets4, dont quatre-vingt-dix pourcents auraient été produits dans les deux

dans leur langage d'animaux, sans que nous soyons nous-mêmes en mesure de répliquer. Même si les concepts d'humain, de non humain ou même d'inhumain n'ont pas cours dans la rationalité algorithmique, il n'en reste pas moins que, parmi les vivants, les êtres humains ont une capacité particulière à résister aux processus de catégorisation et de « nomination » dont ils font l'objet, de rester dans un état de relative indétermination. C'est, précisément, cette indétermination, dans laquelle prend racine le fond d'indécidabilité dans le domaine des affaires humaines, que visent à neutraliser les processus d'optimisation algorithmique des décisions, au profit d'une plus grande efficacité, d'une plus grande opérationnalité, au point que nous pourrions bien être amenés, enfin, exposés comme nous sommes à des formes de catégorisations auxquelles il nous devient impossible de répondre, à faire enfin cause commune avec les animaux.

[3] Draft protocol amending the Convention for the protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

[4] L'octet est l'unité numérique nécessaire pour coder un caractère.

dernières années. Ce nombre, qui double tous les deux ans, devrait être multiplié par dix d'ici 2020, pour atteindre 44 zettabytes[5], ou 44 trillions de gigabytes.[6]

Le phénomène de traduction, ou plutôt de transcription du monde physique et de ses habitants sous forme de données métabolisables par les systèmes informatiques n'est désormais plus limité, ni même freiné de manière essentielle par une inaccessibilité technique ou économique. Si la collecte, le transport et la conservation des données ont bien un coût direct[7], celui-ci décroît en fonction des lois de Moore (doublement de la densité des transistors sur une puce[8] en Silicium tous les 18 mois, augmentant ainsi la capacité de traitement, donc l'efficacité, en permettant, grâce à la multiplication des transistors, le nombre d'opérations complexes prises en charge) et de Nielsen (doublement du débit de connexion tous les 21 mois9). On peut aussi mentionner la loi de Kryder qui prédisait en 2005 que la densité de stockage d'information sur un disque magnétique doublerait tous les 13 mois. En ajoutant à cela l'apparition de nouveaux types de stockage comme les disques SSD, on se rend compte que l'on peut stocker de plus en plus de données et y accéder de plus en plus vite. On assiste donc, à une augmentation exponentielle des capacités de traitement (Moore), de stockage (Kryder) et de communications (Nielsen).

La croissance exponentielle des Big Data résulte de la rétention par défaut non seulement des données directement utiles (dont l'utilité[10] est définie par l'utilisation effective pour une finalité déterminée[11]), mais aussi de celles dont l'utilité a déjà été consommée (qui ne sont plus nécessaires pour la finalité antérieurement fixée), ainsi que de celles qui n'ont d'utilité que potentielle. C'est la quantité (le volume) des données (beaucoup plus que leur qualité) qui permet de trouver une utilité inattendue à toutes sortes de données, y compris les données a priori les moins signifiantes, opérant comme de purs signaux – des signaux individuellement très peu informatifs (on parle parfois de « signaux faibles ») voir même a-signifiants, en provenance du monde connecté. [12]

Ainsi, l'utilité de chaque donnée dépend de la quantité des autres données avec lesquelles elle est susceptible d'être corrélée, plus que de sa densité en information.

---

[5] Un zettabyte correspond à 1,000 000,000,000,000,000,000 bytes, ou octets.

[6] Vernon Turner, John F. Gantz, David Reinsel, Stephen Minton, « The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things », avril 2014, IDC #IDC_1672, étude commanditée par EMC. http://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf

[7] Nous n'évoquerons pas ici les coûts indirects, pour l'environnement et la santé, du développement des technologies numériques.

[8] Ou tous les vingt quatre mois, suivant les versions. La loi de Moore se heurte logiquement, aux limites physiques de la miniaturisation.

[9] http://www.nngroup.com/articles/law-of-bandwidth/

[10] Voir notamment le rapport du Groupe de travail sur l'économie de l'information Groupe de travail sur la sécurité de l'information et la vie privée de l'OCDE, *exploration de l'économie des données personnelles: revue des méthodes de mesure de la valeur pécuniaire des données*, 23 mai 2013, DSTI/ICCP/IE/REG(2011)2/FINAL.
http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/IE/REG(2011)2/FINAL&docLanguage=Fr

[11] Pour une description très claire du phénomène, lire Pierre Delort, Le Big Data, PUF, coll."Que sais-je", 2015.

[12] *Ibid*.

Même des données à très faible densité d'information (des données anonymes qui, individuellement, sont absolument triviales et asignifiantes), gagnent-elles en utilité lorsque leur quantité croît.[13]

Dans l'univers des Big Data, il n'est donc peut-être pas exagéré de penser que, par une sorte d'effet de réseau[14] la valeur potentielle de chaque donnée croisse jusqu'à surpasser, potentiellement, sa valeur actuelle, en fonction de la quantité de données récoltées. Selon certaines estimations répercutées par la Commission européenne, l'accroissement de revenus générés annuellement par les données à caractère personnel des citoyens européens pourrait atteindre, en 2020, une valeur d'un trillion d'euros.15 Cette utilité, ou cette valeur des données n'est bien évidemment ni perceptible ni accessible aux individus qui n'interviennent qu'en tant qu'agrégats temporaires de données « infra-individuelles » exploitables en masse, à l'échelle industrielle. Deux approches s'opposent, dès-lors, s'agissant de la philosophie générale des instruments de protection des données et du « statut » des données personnelles. A l'approche « law and economics », qui est aussi celle des partisans d'un « marché » des données personnelles, qui tendrait donc à considérer les données personnelles comme des « biens » commercialisables, étant donné notamment qu'elles sont effectivement commercialisées (par les entreprises, les courtiers de données,…), et à permettre aux individus de négocier la communication de « leurs » données contre rétribution pécuniaire s'oppose l' approche qui consiste à aborder les données personnelles plutôt en fonction du pouvoir qu'elles confèrent à ceux qui les contrôlent, et à tenter de prévenir de trop grandes disparités informationnelles et de pouvoir entre les responsables de traitement et les individus. C'est, à l'évidence, cette seconde approche qui prévaut en Europe.

1.2. Variété

Une seconde caractéristique des Big Data est leur variété. Outre la variété des formats (textes, images, sons, localisations, trajectoires,….), les données susceptibles d'être enrôlées simultanément dans les analyses de type Big Data émanent d'une multitude de sources et se présentent de manière structurée ou non[16].

[13] C'est ce qui confère d'ailleurs aux grandes plateformes de l'Internet que sont les GAFA (Google, Amazon, Facebook, Apple) des avantages comparatifs indéniables dans l'économie des *Big Data* (bien qu'Apple ait jusqu'aujourd'hui refuse d'entrer dans le *data business*). Ces données ont bien entendu une valeur monétisable: les données sociodémographiques et psychographiques (styles de vie, croyances, valeurs, personnalité) détenues par un réseau social comme Facebook, par exemple, à propos de tous ses utilisateurs, représentent on une valeur économique gigantesque en raison notamment des perspectives qu'elles ouvrent d'une segmentation très fine de la clientèle, ou du ciblage publicitaire.

[14] Un effet de réseau est un phénomène par lequel l'utilité réelle – d'une technique ou d'un produit, par exemple - dépend de la quantité de ses utilisateurs. Transposée dans le domaine des Big data, la théorie de l'effet de réseau donnerait ceci: l'utilité réelle d'une donnée dépend de la quantité des autres données récoltées avec lesquelles elle pourrait être agrégée.

[15] European Commission, "The EU Data Protection Reform and Big Data – Factsheet", avril 2015, http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf

[16] "Les données structurées sont celles dont l'ensemble des valeurs possibles est déterminé et connu à l'avance. Par exemple, dans une base de données rassemblant les résultats d'une enquête d'opinion, l'âge ou la catégorie socio-professionnelle des individus interrogés sont des

Les *hard data* sont produites par les institutions et administrations publiques (données produites lors de recensements, registres de propriété, plaintes et décisions de justice, bilans et faillites, données relatives aux permis de conduire, listes d'électeurs, registres des naissances, des mariages et des décès, des licences de toutes sortes,…). La numérisation des documents publics n'est pas sans incidence sur la vie privée des citoyens. Des documents publics ne relevant pas formellement de la vie privée mais accessibles seulement sous forme d'archives papier étaient, de fait, couvertes par une sorte d'opacité pratique, alors que leur numérisation rend éminemment plus probable leur exposition publique. C'est notamment la raison pour laquelle l'ouverture des données publiques doit impliquer des processus d'anonymisation des données.

Aujourd'hui, lorsque nous, travaillons, consommons, nous déplaçons, nous « produisons » presqu'inévitablement de la donnée.[17] On qualifie de *soft data* les données émises par les individus, soit intentionnellement, à travers les blogs, réseaux sociaux, forums de discussion, soit involontairement, dans la mesure où une part croissante de leurs activités, interactions, trajectoires en ligne ou hors ligne laissent des "traces" digitales qui sont récoltées souvent par défaut à travers des dispositifs de suivi des trajectoires en ligne, de vidéosurveillance, de localisation GPS, de suivi des flux de circulation, d'imagerie satellitaire, d'enregistrement des transactions bancaires,… et conservées à diverses fins, rarement explicitées au moment de la collecte. Si la numérisation du monde ne se heurte à aucune récalcitrance significative des individus c'est en raison du fait qu'elle semble être la contrepartie inévitable, indispensable, indissociable d'une multitude de nouvelles fonctionnalités des appareils numériques, de l'expérience d'une interactivité sociale qui passe par la numérisation, d'un enrichissement du champ perceptif des individus par des informations personnalisées, dynamiques et contextualisées, de nouveaux rapports à soi, à sa santé, à sa productivité, rapport d'autocontrôle et de prévention individuelle passant par l'usage d'appareils numériques de *quantified self* et de santé connectée, d'un certain goût, aussi, pour la surveillance lorsqu'elle étend la sphère de contrôle de l'individu sur ses proches.[18]

---

données structurées, car les tranches d'âges ou la liste des catégories socio-professionnelles possibles sont déterminées a priori. Les réponses libres aux questions ouvertes sont des données non structurées, car ces réponses sont potentiellement toutes différentes et impossibles à catégoriser a priori. Dans une base de données client de mails, l'auteur ou la date sont des données structurées, le corps du message est une donnée non structurée. » (Didier Bourigault, « L'avènement du Big Data révèle la valeur des données non structurées », http://www.synomia.fr/fr/vision-et-techno/synomia-menu-la-data-non-structuree)

[17] Eric Sadin, *surveillance globale. Enquête sur les nouvelles formes de contrôle.* Climats/ Flammarion, 2009.

[18] Note intempestive: Ainsi, il arrive que, sans que cela suscite aucun débat, les parents d'enfants gardés à l'école maternelle exigent de l'instituteur/rice qui s'y plie de bonne grâce qu'il/elle prenne, tout au long de la journée, des photos de leurs enfants et les poste sur une page Facebook dédiée qu'ils pourront, à toute heure du jour, consulter grâce à leur smartphone. Les pratiques sociales numérique d'apparence ludique et convivale dissolvent les murs de l'école au profit d'une ubiquité parentale, et conditionnent la confiance due à l'enseignant à la possibilité de contrôler à tout moment l'état de bien-être des enfants. Au-delà des seuls enjeux de protection de la vie privée et de protection des données à caractère personnel, il s'agira de prendre en compte, en arrière-fond de nos réflexions, les reconfigurations de l'espace social induites par cette nouvelle porosité de contextes précédemment moins perméables aux flux numériques. Dans le domaine de l'enseignement, mais aussi dans celui de l'assurance, de l'emploi, ou même des relations amoureuses, l'exigence de transparence parfaite, de granularité fine et de continuité dans le contrôle, se

A tout cela s'ajoute les *métadonnées*, qui sont – dans le sens le plus général – des 'données à propos des données' – c'est à dire des données, parfois générées automatiquement par les systèmes informatiques eux-mêmes, qui permettent de décrire et de structurer d'autres données, indépendamment de leur contenu. Les métadonnées peuvent, par exemple être des données à propos de la localisation de données, à propos des types de données disponibles, de la provenance des données,[19] … Ce sont, par exemple, les données de trafic, évoquées par la Directive 2002/58/CE du Parlement européen et du conseil du 12 juillet 2002, comme pouvant inclure des données concernant le routage, la durée, le moment ou le volume d'une communication, le protocole de référence, l'emplacement des équipements terminaux de l'expéditeur ou du destinataire, le réseau de départ ou d'arrivée de la communication, ou encore le début, la fin ou la durée d'une connexion. Elles peuvent également représenter le format dans lequel la communication a été acheminée par le réseau. Ce sont aussi les données de localisation, qui peuvent inclure, dans les termes de cette même directive, « la latitude, la longitude et l'altitude du lieu où se trouve l'équipement terminal de l'utilisateur, la direction du mouvement, le degré de précision quant aux informations sur la localisation, l'identification de la cellule du réseau où se situe, à un moment donné, l'équipement terminal, ou encore le moment auquel l'information sur la localisation a été enregistrée. » Plus concrètement, relèvent, par exemple, de la catégorie des métadonnées la date à laquelle une donnée a été produite ou enregistrée, les coordonnées GPS du lieu où une photographie a été prise, la durée d'une communication téléphonique, … Toutes ces métadonnées étaient visées par la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, invalidée par la CJCE le 8 avril 2014.[20] Qu'elles ne doivent plus être obligatoirement conservées pour être mises, le cas échéant, à la disposition des autorités publiques n'empêche bien évidemment pas qu'elles soient éventuellement utilisées, notamment à des fins de réidentification des personnes, ou à des fins de profilage.

Enfin, une part croissante des données numériques provient de ce que l'on appelle d'ores et déjà l'*Internet des objets*[21] : la mise en réseau d'objets « intelligents » capables de communiquer entre eux, et donc de produire, eux aussi, des quantités gigantesques de données.[22] Ces objets en réseau émettent notamment des informations relatives aux trajectoires, aux activités, aux performances, à la consommation énergétique, aux modes de vie,… de leurs usagers.[23]

---

substitue aux asymétries informationnelles induites par les distinctions de rôles, de positionnements, de situation, d'intentions entre les personnes, ou justifiées par l'équité ou l'exigence de solidarité (dans l'assurance). Cette obsession pour la transparence, pour l'accès direct, immédiat, aux données, qui dispense du récit, du rapport, du témoignage, s'accompagne, très paradoxalement, d'un désintérêt pour la compréhension, la maîtrise et l'évaluation (en termes de légitimité, d'équité, de justice), des processus (automatisés) de catégorisation émergeant des traitements de ces données.

[19] Adriaans, P. et Zantinge, D., *Data mining*, Harlow, England: Addison Wesley Longman, 1996.

[20] Arrêt du 8 avril 2014 – Affaires jointes C-293/12 et C-594/12.

[21] En 2015, le nombre de capteurs devrait atteindre 50 billions. (The Internet of Things. How the Next Evolution of the Internet Is Changing Everything, Cisco White Paper, 2011, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf)

[22] http://france.emc.com/leadership/digital-universe/index.htm

[23] cf. Opinion 8/2014 on the on Recent Developments on the Internet of Things

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Toutes ces données sont soit collectées en première main par les administrations ou les entreprises, soit acquises à titre onéreux auprès d'autres administrations ou entreprises, ou auprès de courtiers de données (*databrokers*), aussi appelés courtiers d'informations, revendeurs d'informations, agrégateurs de données ou encore fournisseurs de solutions logicielles et qui font métier de récolter, d'agréger, de fournir des procédés d'analyse et d'exploitation des données massives.[24] Comme les individus n'ont aucune interaction directe avec ces courtiers de données, ils n'ont pas même la possibilité de connaître l'étendue ni la nature des informations collectées et vendues pour une multitude de finalités allant de la prévention des fraudes au marketing en passant par l'évaluation des risques de crédit (*credit scoring*).

Traiter simultanément ces différents types de données est un défi constant pour les praticiens du Big Data. Si les coûts de récolte, de transport et de stockage des données ne cessent de décroître, il n'en va pas de même pour les coûts d'analyse de ces données. Pour acquérir de la valeur, ou de l'utilité – les « données brutes » n'ont en elles-mêmes aucune valeur – les données doivent être traitées. Elles doivent être extraites de leur source d'origine, nettoyées et normalisées, validées avant de pouvoir être réellement exploitées. Transformer les données brutes (existant sous divers formats) en « savoir » opérationnel nécessite des investissements substantiels. La question économique est donc, chaque fois, d'évaluer si la valeur des résultats des analyses fondées sur les Big Data est susceptible de surpasser leur coût.

1.3. Vélocité

Une troisième caractéristique des Big Data est la vitesse à laquelle elles sont accumulées en "temps réel". Jamais les jeux de données n'ont connu une telle flexibilité en extension. Ce qui signifie aussi que l'utilité des données, leur « signification », leur valeur, évolue en temps réel, en fonction de l'afflux de nouvelles données.

Vitesse d'accumulation des données, mais aussi vitesse de traitement des données qui court-circuitent et mettent hors-jeu les processus de perception et d'entendement humains, et les processus d'énonciation des motivations. Ainsi la cible des dispositifs de détection, de classification et d'évaluation anticipative des comportements et propensions humaines (qu'ils soient utilisés dans le domaine de la sécurité, de la lutte anti-terroriste, ou du marketing) n'est pas l'expression ni le début d'exécution des intentions des individus, mais les processus qui les précèdent, souvent à un stade préconscient. (Nous envisagerons, dans la partie de notre rapport consacré à la surveillance numérique et à l'analyse prédictive, les enjeux de ces nouvelles capacités en termes d'autodétermination informationnelle, de droit à la protection de la vie privée en tant qu'elle protège l'individu contre les intrusions excessives dans les processus de développement de sa personnalité, et de garanties contre les discriminations directes et indirectes).

[24] Voir notamment *Data Brokers. A Look at the Canadian and American Landscape*, Report prepared by the Research Group of the Office of the Privacy Commissioner of Canada, 2014, https://www.priv.gc.ca/information/research-recherche/2014/db_201409_e.pdf ; *Data brokers. A Call for Transparency and Accountability*, Federal Trade commission (US), May 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

On pourrait croire que tout ceci n'est que science fiction. Il n'en est rien. Si l'on en croit Eric Schmidt, directeur chez Google, bientôt la technologie deviendra tellement efficace qu'il deviendra très difficile pour les personnes de voir ou consommer quelque chose qui n'aura pas été prévu pour eux.[25] Dans le domaine du marketing, à terme, l'objectif n'est pas tant d'adapter l'offre aux désirs spontanés (pour peu qu'une telle chose existe) des individus mais plutôt d'adapter les désirs des individus à l'offre, en adaptant les stratégies de vente (le moment de l'envoi de la publicité, la manière de présenter le produit, d'en fixer le prix,...), le design de l'interface (de manière à susciter la confiance et l'envie de consommer) au profil pulsionnel de chacun.[26] Ainsi sommes-nous peut-être en train de passer d'une économie de l'intention à une économie de la pulsion. La librairie en ligne Amazon brevetait récemment un logiciel qui lui permettrait d'envoyer les marchandises vers ses clients avant même que ceux-ci n'aient procédé à l'acte d'achat.[27] Les centres d'appel téléphoniques de certaines entreprises, plutôt que d'évaluer les candidats sur la base du *curriculum vitae* et d'un entretien d'embauche, ont recours à des systèmes d'optimisation de la force de travail (c'est l'expression employée par l'industrie du recrutement fondé sur les modélisations produites par les traitements de type Big Data)[28] qui détectent, parmi toutes les informations disponibles sur les réseaux sociaux notamment, non pas directement si le candidat possède les qualités requises mais s'il correspond à certains points de données a priori sans rapport avec les capacités requises par la nature du poste ou de l'emploi (comme le fait d'être inscrit sur deux réseaux sociaux plutôt que sur trois ou sur un seul) mais statistiquement prédictifs d'une bonne performance ou d'une bonne résilience pour le poste vacant,...[29]

Ces dispositifs d' « anticipation performative » des intentions d'achat (qui est aussi un court-circuitage du processus de transformation de la pulsion en désir ou en intention énonçable), d'optimisation de la force de travail fondée sur la détection anticipative des performances futures sur base d'indicateurs produits automatiquement au départ d'analyses de type Big Data (qui signifie aussi une chute vertigineuse du « cours de l'expérience » et des mérites individuels sur le marché de l'emploi), posent des questions innombrables. L'anticipation performative des intentions – et les nouvelles possibilités d'actions *préemptives* fondées sur la détection des intentions, mais de ces intentions - est-elle compatible avec la poursuite de *l'autodétermination* des personnes ? Ne faut-il pas concevoir la possibilité d'énoncer par soi-même et pour soi-même ses intentions et motivations constitue un élément essentiel de l'autodétermination des personnes, contre cette utopie, ou cette dystopie, d'une société dispensée de l'épreuve d'un monde hors calcul, d'un monde où les décisions soient autre chose que l'application scrupuleuse de recommandations automatiques, d'un monde où les décisions portent encore la marque d'un engagement subjectif ? Comment déterminer la *loyauté* de ces pratiques ? L'optimisation de la force de travail fondée sur le profilage numérique est-il compatible avec le principe d'*égalité* et de *non-discrimination* ?

[25] http://online.wsj.com/news/articles/SB10001424052748704901104575423294099527212

[26] A ce sujet, voir Ryan Calo, "Digital Market Manipulation", *George Washington Law Review*, 82, 2014.

[27] Greg Bensinger, "Amazon Wants to Ship Your Package Before You Buy It », *The Wall Street Journal*, 17 janvier 2014.

[28] Voir par exemple *Evolv*, une entreprise qui propose ce genre de logiciel pour l'optimisation de la force de travail: http://www.evolv.net/

[29] Hubert Guillaud, "L'emploi à l'épreuve des algorithmes", *InternetActu*, 3 mai 2013, http://www.internetactu.net/2013/05/03/lemploi-a-lepreuve-des-algorithmes/

1.4. Fiabilité sans vérité : nouvelles logiques de traitement.

Les *Big Data* signifient donc surtout le franchissement d'un seuil de quantité, de complexité, de rapidité de prolifération des données à partir duquel nous serions contraints d'automatiser et d'accélérer (pour tenir compte de l'accroissement continu, à grande vitesse, des masses de données) les processus de transformation des données numériques en informations opérationnelles.[30] L'expression *Big Data* renvoie donc aux masses de données numériques complexes à accumulation rapide, mais aussi à l'ensemble des nouvelles techniques logicielles (Data Mining, Machine Learning, Social Network Analysis, Predictive Analytics, "Sensemaking", Natural Language Processing, Visualization,…) sans lesquelles les données resteraient « muettes », et qui présupposent à leur tour l'utilisation de capacités de stockage et de traitement gigantesques. Cette puissance ne pouvant être offerte par un seul ordinateur, aussi puissant soit-il, on se tourne alors vers la parallélisassions des traitements et des données qui se basent sur l'utilisation simultanée d'un grand nombre de serveurs constitués en grappes (clusters) sur lesquels les données sont distribuées [31] et qui collaborent selon des modèles de calcul distribué [32], à la détection des relations subtiles, qui seraient autrement restées imperceptibles, entre des données très hétérogènes, récoltées dans divers contextes.

Bien sûr, la fiabilité du « savoir » produit par l'analyse des Big Data est tout sauf assurée :

Premièrement, ce n'est pas parce qu'elles ont l'air de « se récolter toutes seules », que les données sont pour autant adéquates et exactes. C'est que la qualité des données et leur adéquation dépend très fortement de la qualité et de la disposition des « capteurs », d'une part, et de la « disposition » des informations pertinentes à se laisser numériser d'autre part. Par ailleurs, la modélisation algorithmique peut, au lieu de neutraliser les biais et préjugés humains, ne faire que les enregistrer et les « naturaliser » (les transformant en « données »), les rendant, en tant que « biais », imperceptibles et incontestables.

- *Une « rationalité immanente »*

Plutôt que de subsumer les données dans des catégories préconstituées (comme les catégories statistiques, dont la construction suppose un processus conventionnel qui peut prendre du temps), les traitements de type Big Data consistent à faire surgir les « catégories » de la masse des données elles-mêmes, quasiment en temps réel. Ces « catégories » algorithmiques, que l'on appelle aussi *patterns*, ou modèles, ou encore profils (lorsqu'elles concernent les comportements humains), sont des « motifs » (on parle d'ailleurs de *visualisation* des données) évolutifs, formés par les corrélations observées non plus dans le monde physique mais entre des données numériques recueillies dans des contextes hétérogènes, indépendamment de toute explication causale. Pour le dire autrement, à la différence des traitements statistiques classiques,

[30] D. Weinberger, *Too Big to Know: Rethinking Knowledge Now That the Facts Aren't the Facts, Experts Are Everywhere, and the Smartest Person in the Room Is the Room*, New York: Basis Books, 2012.
[31] Comme le logiciel Hadoop.
[32] Comme MapReduce.

dans lesquelles les hypothèses ou catégories statistiques précèdent et président à la collecte des données, dans les traitements de type Big Data, c'est exactement l'inverse qui se produit : *la collecte et le traitement des données précèdent et font émerger, des données massives, des hypothèses ou catégories.*

Dès lors, les « modèles », profils ou catégories algorithmiques jouissent d'une aura d'objectivité bien supérieure à celle des catégories statistiques. Comme l'explique très bien Alain Desrosières, [33] les statistiques classiques – parce qu'il faut bien se mettre d'accord sur des critères rendant commensurables, et donc susceptibles d'entrer dans une même catégorie statistique, des événements, performances, phénomènes, hétérogènes - sont le produit de conventions sociales (ce qu'il appelle des conventions d'équivalence, permettant de comparer ce qui, sans elles, serait incomparable), et se présentent donc non comme reflétant objectivement la réalité mais plutôt comme des mises en forme du monde ayant tout au plus une visée de neutralité. Les traitements statistiques impliqués dans l'analyse des Big Data, par contre, visent précisément à dispenser de toute opération conventionnelle, politique, idéologique,… de toute discussion à propos des catégories à travers lesquelles nous percevons le monde, de toute « représentation » du monde puisque les catégories émergent « spontanément » des données elles-mêmes par la grâce d'algorithmes capables de détecter les corrélations statistiquement signifiantes.

Alors que, lorsqu'elles servent de références au débat publique, les objets statistiques « classiques » sont toujours susceptibles d'être remis en question (a-t-on pris assez de données en compte ? n'en a-t-on pas pris trop ?), les modélisations algorithmiques (*patterns* ou profils) semblent a priori devoir échapper à toute forme de remise en question puisqu'elles n'apparaissent plus *produites* ni *construites* mais semblent, au contraire émaner directement du monde numérisé, sans que les jeux de données aient été sélectionnés sur d'autres bases que leur compatibilité technique avec les systèmes d'analyse de type Big Data.

La coextension (postulée par l'idéologie des Big Data) de la base statistique et du réel numérisé est une absorption de ce qui en était exclu par les pratiques statistiques « classiques » : les point trop éloignés de la moyenne (qui pouvait faire dire que les statistiques, ça ne vaut que pour les grands nombres, pas pour les cas individuels), ce qui n'entrait pas « dans les cases » (contre les objets statistiques d'origine conventionnelle, on pouvait toujours argumenter qu'ils n'avaient pas pris assez ou qu'ils avaient pris trop en compte). Tout cela composait un « dehors » pour une pensée la statistique qui avait pour ambition de représenter le monde en certains de ses aspects, et non de s'y substituer. L'incomplétude, la sélectivité de la statistique

[33] Dans un entretien réalisé par Christian Mouhanna, Alain Desrosières expliquait que "Les statistiques sont le produit de conventions sociales. Plutôt que de se demander si elles « reflètent objectivement la réalité », il est plus fécond de les voir comme des mises en forme du monde, parmi d'autres, et de s'interroger sur les procédures d'objectivation. Plutôt que de « neutralité », on pourrait parler de « visée de neutralité » de la part de statisticiens professionnels, de même que Jean Ricœur parle de « visée de réalité » à propos du travail de l'historien. La statistique n'est pas neutre a priori. Seule la reconstitution de ses chaînes de production et d'usage permet de porter un jugement sur sa portée réelle. Les mots « objectivité » et « neutralité » renvoient implicitement à la métrologie des sciences de la nature, alors que les statistiques économiques et sociales peuvent être plus utilement rapprochées du droit et des sciences politiques, dans la mesure où leurs conventions sont des produits sociaux, régis eux-mêmes par des métarègles, elles aussi conventionnelles." (« Entretien avec Alain Desrosières », *Sociologies pratiques* 1/2011 (n° 22), p. 15-18. URL : www.cairn.info/revue-sociologies-pratiques-2011-1-page-15.htm.)

“classique” relativement aux éléments du monde n’est pas à comprendre comme une « faiblesse » de la statistique mais comme une condition indispensable à la « pensée statistique ».

Dans le monde des *Big Data*, l’aura d’objectivité et d’exhaustivité des données numériques, et l’idée répandue suivant laquelle « gouverner par les données » serait une manière de gouverner « objectivement », la perception étant que le sens produit par l’analyse des données, conçues comme purs signaux émanant directement du monde en temps réel, ne serait plus construit socialement, politiquement, culturellement, mais serait l’équivalent d’un dévoilement automatique, hors langage, du monde par lui-même, non interprété, non symbolisé, non représenté, indépendant de toute perspective idéologique est probablement l’une des raisons épistémiques de l’acceptation ou de la tolérance des individus à la numérisation du monde. L’idéologie des *Big Data*, c’est l’utopie d’un accès immédiat, hors langage, au monde. A la crise de la « représentativité » (des catégories statistiques notamment), la numérisation du monde apporte une réponse radicale : il n’y aurait plus rien à représenter, puisque les données, « parlent d’elles-mêmes », d’une façon immanente.[34] C’est donc vers une sorte d’indistinction entre le monde et ses représentations numériques, d’indistinction, aussi, entre la technique et la culture – et donc vers une dépolitisation quantitative - que semble nous orienter l’engouement massif pour les *Big Data*.

Mais l’immanence n’est pas la vérité. Les critères de « véridiction » des modélisations algorithmiques ne sont absolument pas comparables à des critères de véridiction scientifique. La réplicabilité des opérations algorithmiques, par exemple, est quasiment impossible dans un contexte dans lequel les jeux de données impliqués sont en expansion continue. D’ailleurs, ces modélisations dont on peut dire qu’elles sont produites à même le monde numérisé plutôt qu’à propos du monde physique ne visent aucunement à décrire la « vérité » mais seulement à être « opérationnelles ». La question de la validité ne se pose plus en termes de « vérité » mais de « fiabilité » - « reliability without truth », écrit Eric Winsberg[35], une fiabilité réputée d’autant plus grande que les processus sont automatiques et évitent l’intervention humaine - et la dispense de la recherche de la vérité, de même que de l’historicité et de la causalité, est précisément l’un des moteurs de la nouvelle rationalité algorithmique. C’est l’idée de la « boîte noire » : on sait ce qui « entre » d’un côté, on constate ce qui sort de l’autre côté, mais on ne sait pas ce qui se passe entre les deux. Que le monde tel qu’il se produit effectivement ne se conforme pas au modèle produit algorithmiquement, au réel algorithmique – c’est-à-dire, lorsque ce qui arrive dans le monde fait « mentir » le profilage qui en avait été fait – n’est nullement un échec, ni un raté : ces notions d’échec, de raté, n’ont pas de sens dans une réalité numérique où tout écart par rapport à un modèle statistique est immédiatement assimilé dans la base statistique pour servir à affiner le modèle. C’est le principe même de l’apprentissage des machines (*machine learning*), supervisé ou non supervisé.

L’apprentissage est dit « supervisé » lorsque l’algorithme est entraîné sur des données d'apprentissage fournies par le superviseur humain, qui contiennent à la fois les données et les résultats attendus (par exemple: des paramètres médicaux et des

[34] On sait pourtant que les données ne sont jamais « données » mais résultent toujours d’un processus sophistiqué de transcription de la réalité sous une forme métabolisable par les ordinateurs.

[35] Eric Winsberg, “Models of Success versus the Success of Models: Reliability without Truth”, *Synthese*September 2006, Volume 152, Issue 1, pp 1-19.

diagnostics) de manière à permettre son fonctionnement autonome sur des jeux de données pour lesquels les résultats sont inconnus, dans un processus de généralisation. La supervision sert à valider et à (re)calibrer le modèle retenu par l'algorithme (ce qu'il aura détecté comme « bonne » solution) de manière à aider le système à orienter ses modélisations dans la direction désirée.

L'apprentissage est dit « non supervisé », ou bottom-up, lorsqu'on ne fournit pas au système de modèle connu a priori. Aucun jeu de données d'entrainement ne lui est fourni, aucune « bonne solution » ne leur est présentée en modèle. On laisse alors l'algorithme analyser les données et identifier des corrélations entre celles-ci dans l'espoir de voir apparaitre des modèles sous-jacents. Un exemple d'un tel algorithme est celui de groupement, qui permet de faire émerger au sein d'une population des individus 'similaires'.

L'algorithme auto-apprenant est capable de produire des solutions inattendues, des *patterns* ou modèles radicalement neufs, imperceptibles aux sens ordinaires et, en particulier, à l'œil humain (cf. *infra*, p. 41). Bien entendu, l'algorithme doit être entrainé à éliminer les corrélations non pertinentes ou absurdes.[36] Par ailleurs, qu'il n'y ait pas d'hypothèses ou de modèles présidant au travail de l'algorithme ne signifie pas qu'il n'y ait pas d'assomptions, notamment quant aux caractéristiques de l'environnement dans lequel l'algorithme intervient. Ainsi un algorithme qui fonctionnerait sur l'assomption d'un environnement stable, immuable, ne pourra-t-il pas faire face aux changements qui pourraient survenir dans l'environnement, ce qui lui fera produire des solutions incorrectes, non pertinentes ou ineffectives. En particulier, cet algorithme sera incapable de prédire les comportements futurs. Cependant, la croyance en l'objectivité des prédictions algorithmiques, en leur effectivité et en leur opérationnalité court-circuite bien souvent, chez ceux qui les adoptent à diverses fins (prévention de l'insécurité et du terrorisme, détection des propensions à la fraude, prédiction des comportements d'achat, optimisation des ressources humaines,…), le processus d'évaluation critique de ce qui se présente, le plus souvent, comme une recommandation ou un système automatisé d'aide à la décision. Dans la mesure où ces dispositifs automatiques sont achetés et mis en service précisément pour accélérer et objectiver les processus décisionnels, leurs « prédictions » se traduisent souvent quasi automatiquement en actions et interventions, lesquelles, à leur tour, modifient l'état des choses d'une manière qui ne permet plus d'identifier, contrefactuellement, ce qui se serait produit si la recommandation automatique n'avait pas été suivie. Ainsi, l'anticipation ne fait-elle pas que décrire l'avenir, elle le transforme de manière telle qu'il devient extrêmement difficile – par manque de « ground truths » - de « mettre à l'épreuve » les algorithmes auto-apprenants pour évaluer effectivement leur validité épistémologique.

Ainsi pourrait-on dire, à la limite, que le « succès » d'un algorithme se mesure moins à la « vérité » des modèles qu'il produit qu'à la rapidité d'obtention d'informations opérationnelles pour un coût minimum.[37] La logique est celle du rendement, de l'optimisation, pas du tout de la vérité, de la validité, et encore moins de la légitimité.

[36] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law*, Edward Elagar, 2015, p.24.
[37] Jean-Paul Karsenty, "Big data (mégadonnées). Une introduction", *Revue du Mauss permanente* (http://www.journaldu mauss.net), 1er avril 2015)

Cette perte de contestabilité[38] des critères de différentiation entre les individus signifie, *tant pour les individus qui font l'objet de profilages que pour ceux qui se fondent sur ces profilages pour prendre des décisions à l'égard des individus*, un déclin de la responsabilité – une raréfaction des occasions de « répondre » -, allant d'une dispense à une impossibilité de rendre compte des raisons de ses actes ou décisions. Face à ce phénomène, deux voies de solution se profilent : la première – fondée sur l'assomption d'une superposition parfaite entre l'objectivité/la vérité et la justice - consiste à s'assurer techniquement de l'objectivité, du caractère non biaisé, des modélisations algorithmiques (*auditing d'algorithmes*,…).[39] La seconde – fondée sur l'assomption d'une différence/différance fondamentale entre les idéaux d'objectivité et de justice – consiste à exiger la justiciabilité des décisions[40] affectant les individus, quelles soient – ou non – fondées sur des traitements automatisés de données. Il ne s'agit là plus seulement tant de répondre de l'objectivité des processus algorithmiques que du caractère juste, équitable, légitime, des décisions prises en fonction de ces processus. Autrement dit, il s'agit de faire ré-émerger de la « non-nécessité » - sans laquelle il n'est pas de décision (décider réellement présuppose qu'aucune solution ne s'impose par la nécessité), mais seulement de l'obéissance ou du conformisme -, de faire droit à l'incalculable, à l'indécidable par le calcul. Nous tenterons (cf. 2.6 ci-dessous) d'identifier de quelle manière, par exemple, l'inversion de la charge de la preuve dans les cas de suspicion de discrimination indirecte induite par des recommandations automatisées, ou encore l'instauration d'un principe général de justiciabilité des décisions prises sur la base de traitements automatisés (audit d'algorithmes, …) pourraient contribuer à restituer aux individus leurs *capacités à rendre compte, à énoncer par eux-mêmes* de ce qui les fait agir ou décider de telle ou telle manière, cette capacité d'énonciation – avec toutes les capacités de fabulation qu'elle suppose - étant au cœur de la notion de subjectivité juridique peut-être même d'avantage que les capacités d'entendement et de volonté classiquement tenues pour occuper le centre de gravité du sujet de droit.

- *Personnalisation ou individualisation plutôt que catégorisation.*

Un second aspect des traitements de type *Big* data, est lié à la (relative) non sélectivité dans le recueil et le stockage des données : alors que les pratiques statistiques

[38] Antoinette Rouvroy, "The end(s) of critique: data-behaviourism vs. Due process", in Mireille Hildebrandt, Ekatarina De Vries (eds.), *Privacy, Due Process and the Computational Turn.* Routledge, 2012. Available at: http://works.bepress.com/antoinette_rouvroy/44

[39]Voir par exemple l'étude menée par Amit Datta, Michael Carl Tschantz, et Anupam Datta, "Automated Experiments on Ad Privacy Settings A Tale of Opacity, Choice, and Discrimination", Proceedings on Privacy Enhancing Technologies 2015 (1):92–112 http://www.andrew.cmu.edu/user/danupam/dtd-pets15.pdf Dans cette étude, les auteurs mettent par exemple en évidence que le résultat de l'intéraction entre les comportements des usagers, leur déclaration d'être de sex masculin ou feminin dans préférences déclarées dans leurs parameters d' "Ad Settings" et les logiciels de personnalisation des messages publicitaires de Google est que les personnes s'étant déclarées de sexe masculine ont une beaucoup plus grande probabilité que celles qui se sont déclarées de sexe féminin de se voir envoyer des publicités relatives à des professions fortement rémunératrices (publicités pour un coaching de cadres supérieurs).

[40] Dans cette veine, lire notamment Dannielle Keats Citron, Franck Pasquale, "The Scored Society: Due Process for Automated Predictions", *Washington Law Review*, 2014, Vol. 89, 2014, p. 1-; U of Maryland Legal Studies Research Paper No. 2014-8. Available at SSRN: http://ssrn.com/abstract=2376209

« classiques » éliminent des jeux de données tous les « points » de données qui seraient trop éloignés de la moyenne ou du « plus probable » comme générateurs d'erreurs et de perturbations, les traitements de type *Big Data* supposent au contraire de prendre « tout » en compte, y compris ce qu'il y a de plus singulier, de plus éloigné des grands nombres, ces singularités n'étant plus même rapportées à aucune moyenne (la notion même de « moyenne » perdant toute pertinence). C'est ce qui permet des processus de « personnalisation », c'est-à-dire la différenciation en fonction de « profils » (de criminels ou fraudeurs potentiels, de consommateurs, d'utilisateurs,…) de plus en plus nombreux et précis, des interactions sécuritaires, commerciales, administratives, éducatives, médicales,... Cela signifie notamment, en pratique qu'alors que dans le contexte des traitements statistiques traditionnels, on pouvait dire que les statistiques valaient pour les grands nombres, pas pour les cas singuliers, l'approche Big Data, au contraire, vise une pertinence des « catégories » pour les cas les plus singuliers, ou, pour le dire plus simplement, vise à remplacer la catégorisation par la singularisation ou la personnalisation.

Dans la société actuarielle, ou dans la société de l'assurance, la charge correspondant à la part incompressible d'incertitude radicale, qui découle de ce qu'on n'est jamais certains que tout ce qui est possible ou probable se réalise effectivement, est pris en charge par des formes diverses de mutualisation, c'est-à-dire de prise en charge collective, du risque.[41]

Avec l'arrivée des Big Data (mais aussi des phénomènes de *quantified self*), cette mutualisation des risques tend à faire place à une approche beaucoup plus individualisante, tentant de déterminer, grâce notamment à la granularité des analyses de type *Big Data*, pour chacun, individuellement, ses « risques individuels » et ses «coûts réels» - une manière d'individualiser le risque et, du même coup, de détricoter les mécanismes de solidarité devant ce que l'on appelait autrefois « la providence ». Plutôt que de répartir la charge des risques, les politiques *préemptives* consistent à faire, anticipativement *comme si* l'événement redouté avait eu lieu et à prendre immédiatement, par avance, les mesures s'imposant en conséquence (refus d'assurance à un fraudeur potentiel, élimination préventive d'un terroriste potentiel, orientation professionnalisante des enfants sur base d'un profilage précoce,...). Bien entendu, suivant les domaines d'application, la préemption peut être plus ou moins justifiée.

[41] Ainsi François Ewald expliquait-il, à propos du calcul des probabilités au cœur des pratiques des assurances, qu'il fonctionne comme « une ruse de la raison ». Le calcul des probabilités est un instrument d'investigation voué à pallier à l'impossibilité d'expliquer physiquement les phénomènes. C'est un instrument d'expérimentation par la raison pure. Ce n'est pas seulement que nous ignorions les lois régissant les phénomènes que nous percevons dans leur infinie variété et dans leur infinie dispersion, nous ignorons aussi leurs causes. Notre ignorance est telle que, si même nous inférions quelques régularités, nous serions incapables de déterminer si ces régularités seraient constitutives de lois. Le paradoxe du calcul des probabilités résulte du fait que cette ignorance fondamentale n'est pas vouée à être vaincue par aucun savoir qui proviendrait d'une découverte, que nous ne quitterions jamais le domaine de l'observation. Tout l'art du calcul consiste dès lors à faire jouer cette ignorance contre elle-même, de la neutraliser, pourrait-on dire, en l'utilisant contre elle-même. (François Ewald, *Histoire de l'Etat providence*, LGF - Livre de Poche; Nouv. éd. ent. ref (1 janvier 1996), p.114)

Toujours est-il que la fascination pour les *Big Data* et les pratiques de datamining comme moyen d'imputer anticipativement à chacun – d'une manière à la fois très individualisante, singularisante, qui ne passe plus par aucun rapport à aucune « moyenne » calculée sur une population - les coûts et opportunités « réels » dont il est porteur (dans le domaine de la sécurité, de la santé, du marketing, des ressources humaines, de l'assurance, …), n'est peut-être pas tant la conséquence d'un besoin accru de sécurité que d'une transformation de la réponse faite à une demande de sécurité qui, elle, n'est absolument pas neuve.

Dans *Le monde d'hier*, Stefan Zweig, situait dans les années 1900 à Vienne l'âge de la sécurité, l'âge d'or des assurances. A l'âge de la sécurité, on n'avait pas vu disparaître, comme par magie, toute espèce de danger, mais on avait appris, grâce à la statistique, à domestiquer, par le calcul des probabilités et la mutualisation des risques, ce qu'autrefois on eût appelé la providence et qu'on appellerait aujourd'hui l'incertitude.

> "Si je cherche une formule commode qui résume l'époque antérieure à la première guerre mondiale, dans laquelle j'ai été élevé, j'espère avoir trouvé la plus expressive en disant: "C'était l'âge de la sécurité"… Ce sentiment de sécurité était le trésor de millions d'êtres, leur idéal de vie commun, le plus digne d'efforts… peu à peu les grandes masses parvinrent à y accéder. Le siècle de la sécurité devint l'âge d'or des assurances… les domestiques prirent sur leurs économies une assurance vieillesse et payèrent à l'avance à la caisse mortuaire leur propre enterrement."

L'individualisation « parfaite » des risques et opportunités signifierait par exemple la fin de la raison d'être des assurances, dont le rôle premier n'est certainement pas d'individualiser la charge des risques mais au contraire, de constituer des « contrats sociaux » restreints entre des personnes, les assurés, qui, soumis à des risques comparables, s'engagent à prendre en charge collectivement les coups du sort qui s'abattraient sur certains d'entre eux. Comme l'explique François Ewald,

« Il n'y a pas à proprement parler de risque individuel, sans quoi l'assurance se transformerait en gageure ou en pari. Ce n'est en effet que sur l'étendue d'une population que le risque devient calculable. Le travail de l'assureur est précisément de constituer cette population par sélection et division des risques. »[42] Par ailleurs, explique-t-il encore, l'assurance individualise, elle définit chacun comme risque, mais d'une individualité qui ne se réfère plus à une norme abstraite, d'une individualité relative aux autres membres de la population assurée, d'une individualité moyenne ou sociologique. Alors que l'accident, le dommage, la malchance et la souffrance sont toujours individuels, s'abattant sur un individu et épargnant un autre, le *risque* d'un accident, d'un dommage, d'une perte,… affecte toujours – en tant que risque – une population. A proprement parler, il n'existe pas de risque individuel. ; sans quoi l'assurance ne serait rien d'autre qu'un pari. Le risque ne devient quelque chose de calculable que lorsqu'il est réparti sur une population. Le travail de l'assureur consiste, précisément, à constituer cette population en sélectionnant et en divisant les risques. L'assurance ne peut jamais couvrir que des groupes ; elle fonctionne en socialisant les risques. Elle fait de chaque individu une portion du tout.[43]

---

[42] *Ibid*, p.138-139.

[43] François Ewald, « Insurance and Risk » in Graham Burchell, Colin Gordon, Peter Miller (eds.), *The Foucault Effect: Studies in Governmentality*, Chicago University Press, 1991, p. 197-210.

Au regard de ces considérations relatives à l'assurance, les *Big data* permettraient, semble-t-il, le passage d'une société actuarielle à une société post-actuarielle, dans laquelle la solidarité entre personnes relevant de la même « population » d'assurés, est remplacée par la possibilité d'une individualisation et de la fluctuation des primes en temps réel. L'adaptation, en temps réel et en continu, des primes dues par chaque assuré en fonction de son comportement journalier (qualité de la conduite automobile, pratique sportive, habitudes alimentaires,…) pourrait avoir des effets d'incitation (ou de dissuasion) socialement souhaitables, mais pourrait aussi – en permettant par exemple d'évaluer l'état de santé futur des personnes, sur base, par exemple de l'historique de leurs achats de consommation courante (cf. infra) - produire des conséquences néfastes sur le plan des principes d'égalité d'opportunités et de solidarité. A cet égard les enjeux de l'individualisation des primes (ou de l'hyper-segmentation du marché des assurances en fonction d'éléments de plus en plus individuels et singuliers) soulevés par le phénomène des big data ne sont pas foncièrement différents de ceux que soulèvent la mise à disposition des assureurs, employeurs et autres acteurs intéressés des données génétiques individuelles indicatrices de prédispositions à certaines maladies chez des individus actuellement en bonne santé.[44]

Cependant, l'« objectivité » de la constitution algorithmique des profils, ne visant plus *a priori* personne en particulier, ne présupposant plus aucune catégorie perceptuelle, et en cela parfaitement « égalitaires », font aussi des modélisations et classifications fondées sur les Big Data un phénomène en apparence indépendant des systèmes de différenciations juridiques ou traditionnelles (en fonction du statut, de privilèges, d'avantages ou désavantages socio-économiques…) identifiés par Boltanski et Thévenot comme ce sur quoi s'appuie un modèle de cité qui en justifie ou en légitime les « états de grandeur » et dont l'existence est à la fois une condition et un effet des relations de pouvoir[45]. De même, alors que le droit européen, notamment, reconnaît et protège une série de caractéristiques (le sexe, l'orientation sexuelle, le handicap, l'âge, l'origine ethnique, l'origine nationale, et la religion ou les convictions) particulièrement susceptibles d'exposer ceux qui en sont porteurs à des phénomènes de discrimination, les discriminations éventuellement susceptibles d'émerger dans le monde des Big Data seront probablement très difficilement « rattachables » (du moins directement) à ces différentes caractéristiques. En d'autres termes, alors que, par exemple, les directives européennes en la matière visent à prévenir les distinctions de traitement fondées sur la race ou l'origine ethnique, la religion ou les convictions, le handicap, l'âge, le genre ou encore l'orientation sexuelle, cette approche « catégorielle » de la discrimination semble a priori exclure les distinctions de traitement fondées sur l' « intelligence des données », et qui, comme les « machines a-signifiantes » décrites il y a près de trente ans par Félix Guattari, « ne connaissent ni les sujets, ni les personnes, ni les rôles, ni même les objets délimités. C'est précisément ce qui leur confère une sorte de toute-puissance, elles passent à travers les systèmes de signification au sein desquels se reconnaissent et s'aliènent les sujets individués. »[46]

Autrement dit, aux systèmes de perception et d'interprétation du monde précédemment fondés sur des phénomènes de représentation (représentation statistique, témoignage langagier, symbolisation, institutionnalisation,…) et de recognition de structures,

[44] A cet égard, nous nous permettons de renvoyer le lecteur à notre étude sur le sujet. Antoinette Rouvroy Human Genes and Neoliberal Governance: A Foucauldian Critique, Routledge-Cavendish, 2007.

[45] Luc Boltanski et Laurent Thévenot, *De la justification. Les économies de la grandeur*, Gallimard, 1991, p.162.

[46] Félix Guattari, *Révolution moléculaire*, Recherches, coll. Encres, 1977, p. 264.

formes, catégories (politiquement, juridiquement, culturellement) préconstituées, l'hyper-fragmentation et la croissance exponentielle de l'univers numérique substitue la possibilité de modélisations et simultanées plutôt qu'antécédentes aux traitements de données. Pour cette raison, la reconfiguration radicale de ce que Michel Foucault appelait les « pratiques divisantes »[47] (présidant au distinctions de traitement opérées entre les individus) par les traitements de type Big Data défie - plus fondamentalement encore que les régimes de protection de la vie privé et des données personnelles - le droit de la non-discrimination, lequel a toujours été pensé en fonction de la préexistence de catégories, de groupes humains préconstitués, clairement reconnaissables et à ce titre particulièrement vulnérables aux pratiques discriminatoires[48].

1.5. Conclusion de la première partie.

Evoquer les *Big Data*, c'est évoquer d'emblée un changement d'approche dans la détection, la classification, l'évaluation anticipative des événements du monde et des comportements et propensions de ses habitants, c'est-à-dire, donc, une nouvelle manière de rendre le monde « prévisible »[49] à défaut de le rendre « signifiant » (se passant des processus d'énonciation et de véridiction classiques) articulée à de nouveaux modes d'exercice du pouvoir : une nouvelle « gouvernementalité »[50]. Dans la mesure où l' « intelligence des données », ravivant une sorte de comportementalisme numérique, supplanterait progressivement les formes – statistiques, politiques, juridiques,…- à travers lesquelles nous nous représentons le réel, il convient de se demander comment le Droit serait encore en mesure de contenir, de borner, de limiter l'emprise d'une gouvernementalité algorithmique, y compris sur les processus législatifs et judiciaires.

Evoquer les Big Data c'est aussi évoquer d'emblée de nouvelles perspectives d'innovation technologique, de nouveaux services, de plus en plus personnalisés, capables d'anticiper plutôt que de seulement réagir aux stimuli du monde numérisé. Il est d'ailleurs frappant de constater qu'à l'égard de ce qu'il est convenu d'appeler la « révolution numérique », sans doute en raison de l'accession d'un « impératif

[47] "(…) j'ai étudié l'objectivation du sujet dans ce que j'appellerai des "pratiques divisantes". Le sujet est soit divisé à l'intérieur de lui-même, soit divisé des autres. Ce processus fait de lui un objet. Le partage entre le fou et l'homme sain d'esprit, le malade et l'individu en bonne santé, le criminel et le « gentil garçon » illustre cette tendance. » (Michell Foucault, « Le sujet et le pouvoir », *Dits et Ecrits II*, Gallimard, 2001, p.1042.

[48] Nous verrons que les approches Big Data questionnent l'efficacité de l'approche actuelle consistant à interdire et à empêcher les distinctions de traitement fondées sur des caractéristiques protégées ou catégories vulnérables d'une part, et en empêchent toute action collective des victimes potentielles de discriminations fondées sur le profilage algorithmique d'autre part.

[49] Mais il faudrait trouver un autre adjectif que "prévisible" dans la mesure, d'une part, où le rapport au monde induit par les Big Data dispense de tout rapport "sensible" (de tout rapport visuel, en particulier) au monde et, d'autre part, où il ne s'agit plus tant de prévoir en vue de prévenir que de détecter dans l'actuel de pures potentialités et d'agir "par avance" comme si celles-ci étaient "réalisées" ou "actualisées". Il ne s'agit donc plus tant de "réagir" à des "stimuli" du monde que d'anticiper les événements du monde en produisant les stimuli adéquats.

[50] A propos de la notion de gouvernementalité, voir Michel Foucault, "La gouvernementalité", In *Dits et écrits*, t.II, Paris, Gallimard, Quarto, 1994, 635–657 ; Graham Burchell, Colin Gordon, Peter Miller, eds. *The Foucault Effect. Studies in Governementality*, U. Chicago Press, 1991.

d'innovation » au statut de logique absolue, les individus se trouvent, le plus souvent, qualifiés de « consommateurs » ou d'« utilisateurs » dont on promet d'améliorer l'expérience, et beaucoup plus rarement interpellés en tant que « citoyens ».

Certaines parties prenantes soutiennent qu'afin de favoriser l'innovation et la réalisation du potentiel économique que représentent les big data l'application de certains principes fondamentaux de la protection des données (les principes de finalité, de minimisation des données, en particulier) devraient être assouplis au profit d'une approche « risk-based » (fondée sur le risque). L'idée serait de libéraliser considérablement la collecte des données pour en règlementer plutôt l'usage dans une perspective fondée sur l'anticipation des préjudices possibles (harm-based) de nature à promouvoir un usage responsable des données. Pourtant, comme le déclarait récemment le groupe de travail de l' « article 29 »[51] il n'existe pas aujourd'hui de raison convaincante de penser que les principes fondamentaux de protection des données ne soient plus valides et applicables dans le contexte des Big Data, moyennant certaines améliorations de nature à les rendre plus effectifs en pratique. Le groupe "article 29" explique en outre que le respect du régime de protection des données est un élément fondamental pour créer et conserver la confiance dont toutes les parties prenantes ont besoin pour pouvoir développer des modèles d'affaires fondés sur l'analyse de ces données. En outre, rappelle le groupe de l'article 29", le respect des règles de protection des données et le développement de solutions "privacy-friendly" est essentiel pour assurer une concurrence équitable et effective entre acteurs économiques sur les marches pertinents. En particulier, soutenir le principe de finalité est essentiel pour éviter que des entreprises en situation de monopole ou en position dominante avant l'avènement des Big Data ne conservent un avantage excessif au détriment des nouveaux entrants sur ces marchés.

Dans un premier temps, les attentes générées par le phénomène des Big Data convergent vers la perspective d'amélioration (dans le sens d'une objectivation et d'une optimisation) des décisions dans une multitude de secteurs : sécurité et prévention du terrorisme, optimisation et distribution de la présence policière, soins de santé, politiques énergétiques, gestion du trafic et optimisation des transports en commun, prévention des fraudes, marketing et amélioration de l' « expérience des utilisateurs ou des consommateurs », différenciation des prix en fonction des profils des consommateurs, gestion des stocks, gestion du trafic, orientation en éducation et formation, recrutement et gestion des ressources humaines…).

Les Big Data induisent par exemple de nouvelles attentes en termes de planification « objective » des politiques publiques. Collectées notamment à travers tous les capteurs impliqués dans le déploiement du concept de ville intelligente et à travers les appareils de téléphonie mobile, les Big Data promettent de pouvoir prendre la mesure objective, en temps réel, de la vie urbaine et de ses infrastructures, au profit d'un développement, d'une gestion, d'une réglementation et d'une vie dans la ville fondées sur les données – donc sur une forme numérique, quantitative d'évidence rationnelle. Les Big Data pourraient par exemple permettre d'optimiser la fréquence, les horaires et les trajectoires des véhicules de transports en commun en fonction des intérêts collectifs déduits de la géolocalisation.

[51] Déclaration du Groupe "article 29" du 16 septembre 2014 sur l'impact du développement des données massives sur la protection des individus eût égard au traitement de leurs données à caractère personnel dans l'Union européenne. (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf)

Cependant, les nouvelles capacités de surveillance numérique, d'analyse préemptive et de décision automatisée accompagnant le tournant computationnel[52] ravivent aussi, crucialement, la question fondamentale de la définition du pacte social existant entre les individus, les entreprises et les Etats.[53] La présentation des enjeux en termes d'innovation, de compétitivité, d'intérêts individuels des consommateurs ou des utilisateurs occulte bien souvent les enjeux éthiques, juridiques, politiques, de la révolution numérique au risque de porter atteinte à la prééminence du droit ainsi que des droits de l'homme et des libertés fondamentales, et d'empêcher la recherche d'un juste équilibre entre intérêts privés et publics d'une part, et entre ces intérêts et les droits et libertés en jeu d'autre part. Cependant, les capacités nouvelles fondées sur « l'intelligence des données », dont beaucoup restent imperceptibles ou inaccessibles au citoyen ordinaire, peuvent aggraver considérablement l'asymétrie d'information et/ou de pouvoirs entre ceux qui détiennent les données et ceux qui, volontairement ou non, les « émettent ».

Or l'une des « valeurs ajoutées » du droit fondamental à la protection des données à caractère personnel, par rapport au droit fondamental à la protection de la vie privée est précisément d'avoir parmi ses objectifs de réduire les asymétries de pouvoir et les asymétries d'information entre les individus et les personnes physiques ou morales qui collectent, conservent et traitent les données qui leur sont relatives.[54]

Philip Agre donnait des objectifs poursuivis par les instruments de protection des données d'une part, et les instruments de protection de la vie privée d'autre part, une description assez convaincante :

« La protection des données confère à l'individu un certain contrôle sur l'ampleur et la manière dont certains aspects de son identité sont exposés au monde, alors que la protection de la vie privée garantit la possibilité, pour l'individu, de construire sa personnalité à l'abri de contraintes extérieures excessives »[55].

Ainsi, afin de « conférer à l'individu un certain contrôle sur l'ampleur et la manière dont certains aspects de son identité sont exposés au monde », le droit à la protection des données à caractère personnel garantit à l'individu des prérogatives de contrôle sur les données qui lui sont relatives (une certaine *autodétermination informationnelle*) quand bien même leur traitement ne constituerait pas une atteinte au droit à la protection de la vie privée : la notion de donnée à caractère personnel inclut notamment les données

[52] La métaphore du "tournant computationnel" évoque une certaine transformation du "tournant linguistique": l'unité de perception, de compréhension du monde n'est plus la phrase, le mot, le signe, toujours porteurs de significations, mais la donnée, fragment individuellement asignifiant mais calculable, transpiration plutôt que transcription du monde, degré zéro de l'écriture si l'on puis dire.

[53] Nous n'évoquerons pas ici les questions relatives à la transition vers une économie du partage (crowdsourcing) qui, elles aussi, questionnent la nature du pacte existant entre individus, entreprises et Etat.

[54] Orla Lynskey, Orla, "Deconstructing data protection: the 'added-value' of a right to dataprotection in the EU legal order". *International and Comparative Law Quarterly*, 63 (3), 2014, pp. 569-597.

[55] Philip E. Agre, Marc Rotenberg (eds.), Technology and Privacy. The New Landscape, MIT Press, 1998, p. 3. A propos de la distinction entre le droit à la protection de la vie privée et le droit à la protection des données à caractère personnel, voir aussi Juliane Kokott et Christoph Sobotta, « The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR », *International Data Privacy Law*, 2013, 3 (4): 222-228. A propos de l'éclipse, par le droit à la protection de al vie privée, du droit à la protection des données à caractère personnel dans le droit de l'Union européenne, Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014.

relatives à des personnes non identifiées mais identifiables, qu'il soit effectivement procédé ou non à l'identification de ces personnes (alors que la constatation d'une violation du droit à la vie privée présupposerait au minimum que la personne soit identifiée)[56].

Eût égard au rôle de la protection des données à caractère personnel dans la société[57], notamment en vue de lutter contre toutes les formes de discrimination, compte tenu de la nécessité de concilier la protection des données avec d'autres droits et libertés fondamentaux et de la nécessité de prendre en compte le caractère indivisible des droits civils et politiques et des droits économiques, sociaux et culturels, nous proposons d'évaluer, dans une seconde partie, la contribution que pourrait offrir la Convention 108 du Conseil de l'Europe à la protection de toutes les personnes physiques à l'égard du traitement de données impliquées dans les Big Data.

[56] Friedl v Austria (1996) 21 EHRR 83.

[57] La Cour de Justice de l'Union européenne, se référant à son arrêt du 12 juin 2003, Schmidberger (C-112/00, Rec. p. I-5659, point 80), rappellait à juste titre, dans son arrêt du 9 novembre 2010, concernant les affaires jointes C-92/09 et C-93/09, Volker und Markus Schecke GbR et Hartmut Eifert (Rec. 2010, p. I-0000), que le droit fondamental à la protection des données à caractère personnel, "n'apparaît (…) pas comme une prérogative absolue, mais doit être pris en considération par rapport à sa fonction dans la société".

2. LA CONVENTION 108 DU CONSEIL DE L'EUROPE A L'ERE DES BIG DATA.

2.1 Champ d'application et définitions (article 2.a.) - La notion de donnée à caractère personnel.

Les **données à caractère personnel** (toute information[58] concernant une personne physique identifiée ou identifiable) – qui sont les seules dont les traitements automatisés (ou non) nous ont parus suffisamment menaçants pour les droits et libertés fondamentaux pour justifier un encadrement législatif – n'interviennent pas toujours dans les traitements de type *Big* Data.

Il est des applications, qui visent par exemple l'analyse climatique ou le contrôle des plateformes pétrolières à partir des données recueillies par les capteurs disposés sur leurs équipements techniques, qui n'impliquent à aucun moment le traitement de données à caractère personnel. Les applications visant, par exemple, à prédire la survenance et le déploiement d'épidémies (*Google Flu*), à découvrir les effets secondaires de médicaments ou à combattre la pollution dans les grandes villes, n'impliquent pas le traitement de données à caractère personnel pourvu que les données aient été soigneusement anonymisées.

Il arrive aussi que les données à caractère personnel interviennent de manière évidente dans les traitements *Big Data.* Dans ces cas, les données peuvent provenir des applications de téléphones mobiles, des *smart grids*, des transpondeurs intégrés aux véhicules et servant à calculer des taxes au kilomètre ou à faire varier le montant des primes d'assurance en fonction des distances parcourues, des dossiers médicaux, des données de localisation, des réseaux sociaux, des registres de passagers des transports aériens, des registres publics, des programmes de fidélité, des séquençages génomiques, des historiques d'achats, mais aussi, de plus en plus, d'une quantité d'objets « intelligents » (brosses à dent, réfrigérateurs, chaussures, montres, télévisions,…) qui permettent non seulement d'identifier leurs propriétaires mais sont en plus très révélatrices de leurs modes de vie.[59]

Dans ces cas, l'**anonymisation** des données est présentée comme une condition suffisante pour dispenser les responsables des traitements des obligations qui leur sont imposées et à priver les individus des prérogatives qui leur sont garanties au titre de leur droit à la protection des données à caractère personnel. Cependant, comme le faisait remarquer le Groupe de travail « article 29 » dans son avis du 10 avril 2014 sur les techniques d'anonymisation, "[L'] anonymisation constitue un traitement ultérieur des données à caractère personnel; à ce titre, elle doit satisfaire à l'exigence de compatibilité au regard des motifs juridiques et des circonstances du traitement

[58] A titre préliminaire, la question pourrait se poser de savoir si une donnée, prise isolément, est une information, ou si elle est "seulement" un signal dépourvu de signification mais quantifiable. L'information, en ce cas, serait le résultat du traitement des données.

[59] International Working Group on Data Protection in Telecommunications, Working Paper on Big Data and Privacy. Privacy principles under pressure in the age of Big Data analytics, 55th Meeting, 5 – 6 May 2014, Skopje.

ultérieur. De plus, si les données anonymisées sortent du champ d'application de la législation sur la protection des données, les personnes concernées peuvent néanmoins avoir droit à une protection au titre d'autres dispositions (comme celles qui protègent la confidentialité des communications)."[60]

Deux questions, essentiellement, se posent dans le contexte des Big Data. Premièrement, la distinction entre données personnelles / données anonymes n'est plus évidente alors que les possibilités de réidentification des individus sur base de données anonymes est un risque considérable. Deuxièmement, l'anonymat ne garantit pas contre les possibilités de caractérisation des comportements des individus, ni contre l'analyse prédictive de ces comportements.

- *Les risques de réidentification des individus « par croisement » de données anonymes.*

Dans le contexte des Big Data, comme le montre notamment une étude récente de chercheurs du MIT, il suffit, pour d'identifier 90 pourcent des personnes dans un jeu de métadonnées anonymes (ne contenant aucun nom, aucune adresse, aucun numéro de carte de crédit ni rien d'autre qui puisse être considéré comme donnée personnelle) concernant à trois mois de transactions effectuées par 1,1 million d'utilisateurs de cartes de crédit, de disposer de quatre données spatiotemporelles. La connaissance du montant d'une seule transaction augmenterait le risque de réidentification de 20% montrent-ils encore. Une étude précédente avait montré le même phénomène de réidentifiabilité au départ de données de localisation anonymes.[61]

Ces possibilités de réidentification au départ de métadonnées anonymes tiennent au fait tout à fait trivial que chaque individu présente certaines régularités de comportement, qui, peut-être échappent à sa propre perception, mais sont facilement repérables à travers ses « traces numériques » pour autant que celles-ci soient récoltées et conservées pendant un certain temps (trois mois pour les études susmentionnées). L'anonymat, dans un contexte de Big Data, est donc une réalité toute relative, dépendante de la quantité, de la variété et du temps de conservation des données beaucoup plus que de la « densité en information » de chaque donnée.

a) Face à ces risques substantiels de réidentification existant relativement aux données anonymes, faudrait-il considérer que les données anonymes devraient être considérées comme des données à caractère personnel dès lors qu'elles interviennent dans des traitements de type Big Data de nature à affecter les opportunités socio-économiques d'une personne ? Cette solution se heurte à une série d'obstacles pratiques. Comment, en effet, déterminer le « moment » à partir duquel ne donnée

[60] Voir l'Avis 05/2014 du groupe de travail de l'article 29 sur les techniques d'anonymisation: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

[61] Yves-Alexandre de Montjoye, « Unique in the shopping mall: On the reidentifiability of credit card metadata », *Science*, n° 347, 30 janvier 2015 ; Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen et Vincent D. Blondel, « Unique in the Crowd: The privacy bounds of human mobility », *Nature SRep*, n° 3, 25 mars 2013.

anonyme commence à contribuer à la création d'un « profil » ? Comment, aussi, identifier *a priori* (c'est-à-dire avant que la finalité de profilage soit réalisée) la personne physique « titulaire » des données ?

b) Une autre approche, plus praticable, consisterait à contraindre les entités qui souhaitent anonymiser des données à procéder à l'évaluation préalable des risques de réidentification (en fonction de la quantité, de la variété et du temps de conservation envisagée pour les données récoltées), et à en communiquer les résultats aux individus préalablement au recueil de leur consentement mais aussi, à tout moment, en cas d'accroissement du risque de réidentification. Cette solution se place dans la perspective plus générale de l'exigence de l'étude d'impact préalable sur la protection des données et la vie privée (*privacy impact assessment*) et de l'exigence de l'adoption de mesures techniques et organisationnelles prenant en compte les implications du droit à la protection des données à caractère personnel à tous les stades du traitement des données prévues à l'**article 8bis§2 et §3** (obligations complémentaires) de la Convention 108 (modernisée). Cette solution est loin d'être parfaite, bien entendu. Une difficulté tient notamment à la dimension temporelle de la problématique de la réidentification. Des données aujourd'hui anonymes risquent de perdre ce caractère dans l'avenir en raison d'un possible croisement de ces données avec d'autres données, entre les mains du responsable du traitement de ces données anonymes ou entre les mains de tiers. Le risque de réidentification est éminemment évolutif dans le temps. L'analyse de risques ne peut donc être faite une fois pour toutes, elle doit faire l'objet d'une réévaluation régulière, ou d'un « monitoring » constant, ce qui est d'autant plus difficile qu'est difficilement envisageable la réalisation d'un « inventaire » de toutes les données, actuelles et futures, susceptibles d'être « croisées » avec les données anonymes en la possession du responsable du traitement.

Néanmoins, bien qu'insuffisante, l'exigence d'une analyse de risques au moment de l'anonymisation, éventuellement assortie d'une exigence de réévaluation régulière, offre l'avantage de sensibiliser tant les personnes concernées que les responsables de traitement au fait que l'anonymat n'est jamais garanti et de les inciter des lors à la prudence lorsque, pour les premiers, ils émettent un consentement, et, pour les seconds, ils rendent possible le croisement des données anonymes en leur possession avec d'autres jeux de données en leur possession également ou en la possession de tiers.

En tous les cas, le seul argument suivant lequel les données traitées sont des données anonymes ne devrait pas suffire à immuniser les responsables du traitement de toute responsabilité mais au contraire, étant donnés les risques de réidentification, ils devraient être obligés notamment de prendre toutes les mesures techniques susceptibles de minimiser ces risques. [62]

- *L'anonymat ne garantit pas contre les possibilités de caractérisation des comportements des individus, ni contre l'analyse prédictive de ces comportements.*

Comme les « modèles » ou « profils » sont construits au départ de données en provenance de grandes quantités d'individus, et que les données relatives à l'un des individus sont tout aussi (peu) signifiantes que celles d'un autre pour la modélisation,

[62] Voir également Arvind Narayanan Joanna Huey Edward W. Felten, « A Precautionary Approach to Big Data Privacy », March 19, 2015, CPDP proceeding, http://randomwalker.info/publications/precautionary.pdf

des données très peu personnelles, en très petite quantité, suffisent à produire à l'égard de n'importe quel individu des savoirs « nouveaux », c'est à dire à inférer certains éléments sans rapport immédiat avec les données « qui le concernent » mais qui permettent néanmoins de le « cataloguer »[63]. Autrement dit, pour construire un « profil » - afin de pouvoir « capitaliser » sur les risques et opportunités dont nous sommes porteurs - les données de nos voisins sont aussi bonnes que les nôtres. Faudrait-il concevoir, des lors, que chaque individu soit titulaire des données relatives à ses voisins dans la mesure où leur récolte et leur traitement risque de permettre de la caractériser elle-même ou de l'affecter d'un profil particulier ? Cela signifierait notamment que les mêmes données puissent être revendiquées par de nombreuses personnes comme « leurs » données à caractère personnel, ce qui serait bien entendu absolument ingérable.

Cette nécessité de rapporter les enjeux à des questions de protection des données personnelles témoigne d'un individualisme méthodologique qu'il serait peut-être bon de dépasser relativement à la problématique qui nous occupe. Les formes de pouvoir qui s'exercent dans le contexte des *Big Data* passent peut-être beaucoup moins par les traitements de données à caractère personnel et l'identification des individus que par des formes algorithmiques de catégorisations impersonnelles, évolutives en continu, des opportunités et des risques, c'est-à-dire des formes de vie (attitudes, trajectoires,…). Un profil, ce n'est en réalité personne – personne n'y correspond totalement, et aucun profil ne vise qu'une seule personne, identifiée ou identifiable. Pourtant, être profilé de telle ou telle manière, affecte les opportunités qui nous sont disponibles et, ainsi, l'espace de possibilités qui nous définit : non seulement ce que nous avons fait ou faisons, mais ce que nous aurions pu faire ou pourrions faire dans l'avenir.[64] De plus, comme nous l'avons montré plus haut, la valeur de chaque donnée n'est plus, dans le contexte des *Big Data*, contenue en elle-même, mais est essentiellement de nature relationnelle: ce sont les (cor)relations entre données qui leur confèrent une utilité, une valeur, et aussi, éventuellement, un caractère plus ou moins sensible.

Le défi qui serait le nôtre aujourd'hui pourrait donc s'énoncer ainsi: comment tenir compte, dans les instruments de protection des données personnelles, de la nature relationnelle, et donc aussi collective, de ce qui, à travers les données, mérite d'être protégé ?

2.2 Principes de base : licéité et bonne foi, finalité et proportionnalité, exactitude.

- *Consentement (**article 5§2**)*

En vertu de **l'article 5§2** de la Convention 108 du Conseil de l'Europe (modernisée), le traitement de données ne peut être effectué que sur base du **consentement** libre, spécifique, éclairé et non équivoque de la personne concernée ou en vertu d'autres fondements prévus par la loi.

[63] Martijn van Otterlo, « Counting Sheep: Automated Profiling, Predictions and Control », contribution à l'*Amsterdam Privacy Conference* des 7-10 octobre 2012.
[64] A cet égard, voir Ian Hacking, "Making Up People", *London Review of Books*, 2006, vol.26, no.16, pp. 23-26.

Par rapport aux données à caractère personnel impliquées dans des traitements de type *Big Data*, le caractère protecteur de l'exigence du consentement spécifique, libre et éclairé risque de perdre en effectivité[65] des lors que le consentement au recueil et au traitement de ces données intervient contractuellement comme pré-condition à l'utilisation de certains appareils, services ou applications (souvent présentés comme des contrats d'adhésion), ou des lors que certains appareils connectés seraient offerts gratuitement à condition que leurs utilisateurs consentent à la collecte et au traitement des données personnelles captées par ces appareils. C'est en termes d'acceptabilité de la renonciation au droit à la protection des données à caractère personnel – un droit reconnu comme fondamental - que se pose dès lors la question plutôt qu'en termes de consentement éclairé.

Outre cela, il semble que les individus, la plupart du temps, consentent sur un mode quasiment automatique à la collecte systématique de ces *soft data*. Cet état de fait est dû à une série de facteurs : l'argument suivant lequel « qui n'a rien à cacher n'a rien à craindre de la surveillance », ajouté au confort de l'immédiateté, aux vertus de l'interaction et à la valorisation de l'exposition personnelle l'emportent largement sur les réticences au dévoilement de la vie privée et à la communication des données personnelles. C'est d'autant plus vrai que l'effacement de ses traces digitales demande – lorsque les "architectures de choix" impliquent des règles d'enregistrement par défaut (*opt-out*), comme c'est souvent le cas - de la part de l'individu, une démarche active.

A cet égard, le *succès* des règles de conservation des données par défaut ou, pour le dire autrement, le manque de succès des options permettant de déroger à cette règle de conservation des données tiendrait, si l'on en croit Cass R. Sunstein[66], se fondant sur l'économie comportementale, à la combinaison de trois facteurs principaux. Le premier facteur est l'inertie des comportements des lors qu'effacer « ses traces » demande un effort dont on ne sait au juste s'il vaut vraiment la peine, étant donné que chacune des données émanant de nos activités en ligne nous paraît à nous-mêmes, *a priori* (indépendamment des opérations de recoupement, de croisement, de modélisation auxquelles elles pourraient contribuer), de peu d'importance. La règle par défaut, quand bien même nous avons la possibilité d'y déroger très facilement « en quelques clics » prévaudra toujours lorsque l'enjeu ponctuel, actuel, n'apparaît pas significatif aux yeux de l'internaute. Le second facteur favorisant la règle de conservation par défaut consiste en ceci que, dans une situation d'incertitude quant à la marche à suivre, l'utilisateur moyen aura tendance à considérer que la règle par défaut, puisqu'elle a été pensée par d'autres que lui, réputés plus experts et puisqu'elle est probablement suivie par la plupart des autres personnes, est sans doute la meilleure option pour lui aussi. Enfin, le troisième facteur consiste dans le fait que les individus soient généralement plus sensibles au *risque de perdre* un avantage dont ils ont ou croient avoir la jouissance en se maintenant dans la situation dans laquelle ils se trouvent qu'à *l'opportunité de gagner* quelque chose en changeant. C'est une variante du phénomène d'inertie mais à travers laquelle les concepteurs, des « designers », les « marketeurs » peuvent avoir une prise sur les individus : ils peuvent réduire la probabilité que les utilisateurs s'écartent de la règle par défaut dans

[65] Pour une critique du principe du consentement dans le contexte de la modélisation prédictive des comportements fondés sur les analyses de type Big Data, voir Mantelero, A. The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics. Computer Law and Security Review 2014, (30):643-660.

[66] Cass R. Sunstein, « Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules : A Triptych », 19 mai 2013, http://ssrn.com/abstract=2171343

l'ajustement des « règles de confidentialité » en évoquant tout ce qu'ils ont à perdre dans la mesure où la rétention des « traces numériques » est ce qui permet de leur offrir un service plus personnalisé, plus adapté à leurs besoins en temps réel en fonction du lieu où ils se trouvent, ou de leurs goûts, un service plus rapide et efficace, et que l'effacement leur fera *perdre* tous ces avantages suffira généralement à éviter que l'utilisateur ne s'écarte de la règle par défaut.

Une étude récente[67], cependant, suggère que le « consentement » des internautes à la collecte et à la conservation des données transpirant de leurs activités en ligne ne relèverait pas tant de le fait qu'ils auraient l'impression d'y trouver leur compte, en acceptant de troquer les données transpirant de leurs activités en ligne en échange d'avantages (en termes de ristournes, par exemple), comme aiment à le faire croire le secteur du marketing, que d'un sentiment de résignation face à une sentiment de perte de contrôle inévitable sur les données, un sentiment renforcé si pas induit par les proclamations de la « fin de la vie privée » émanant essentiellement par certains grands acteurs de l'Internet qui ont intérêt à cette résignation des internautes et copieusement amplifiées par les médias.

Toujours est-il qu'en raison notamment des réglages par défaut des appareils numériques et des logiciels d'applications (qui conservent par exemple l'historique des recherches sur les moteurs de recherche à moins que l'utilisateur ne manifeste expressément sa volonté de ne pas conserver d'historique), c'est plutôt sur le mode de l'adhésion par défaut que du consentement libre et éclairé que les individus vivent cette prolifération des données enregistrées « dans les nuages », c'est-à-dire très loin de l'appareil de l'utilisateur, mais, contrairement à ce qu'évoque la métaphore nébuleuse, non pas de façon distribuée mais dans d'une manière très centralisée dans de gigantesques entrepôts de données *(datacenters)*.

Parce que l'autonomie individuelle, pour peu qu'elle existe, n'est pas une capacité purement psychique, mais qu'elle dépend de facteurs socio-économiques, éducatifs, de « design », les « architectures » du choix individuel – telles que les systèmes de règles par défaut - fondées sur des acquis de la psychologie sociale ou sur une détection algorithmique du profil psychologique de celui qu'on appelle l'utilisateur, devraient faire l'objet d'évaluations rigoureuses, spécialement lorsqu'elles sont l'œuvre d'acteurs dont les intérêts ne sont pas alignés sur ceux des « utilisateurs ». Nous ne saurions trop insister sur l'urgence de procéder à une typologie des acteurs du « numérique » et surtout de leurs « intérêts ». Cette voie nous semble plus prometteuse à l'heure actuelle qu'un arc-boutement de principe sur l'exigence illusoire d'un consentement libre et éclairé.

Les architectures de choix construites par des acteurs dont les intérêts ne sont pas alignés sur ceux de l'utilisateur, incitant, par les moyens décrits plus haut, l'utilisateur à ne pas s'écarter de la règle par défaut, d'être en pratique incompatible avec ce qu'Henri Atlan, par exemple, appelle « l'expérience minimale du choix » qui

> « implique que plusieurs alternatives soient offertes et *que le choix soit le facteur déterminant* par lequel l'une d'entre elles est réalisée, passant ainsi du statut de possible à celui de réel, ou, plus précisément, d'actuel."[68]

[67] Joseph Turow,.Michael Hennessy,.Nora Draper,."The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation," *A Report from the Annenberg School for Communication, University of Pennsylvania*, June 2015.
[68] Henri Atlan, *Les étincelles de hasard,* T. 2., Seuil, 2003, *p*. 77.

De ce qui précède (la facilité des *Trade offs* consistant à consentir au traitement des données en échange d'avantages divers et le « pouvoir des architectures de choix » sur les décisions individuelles) il ressort que l'exigence du consentement est très peu protectrice des intérêts individuels et collectifs éventuellement menacés par des traitements massifs de données personnelles. Dès lors, il conviendrait de spécifier plus avant les conditions d'un consentement « libre, spécifique, éclairé et non équivoque » en précisant notamment que les responsables de traitement doivent garantir que le choix de l'individu soit le facteur déterminant (à l'exclusion des offres d'avantages de toute nature en échange du consentement, et à l'exclusion de toute manipulation de l'architecture de choix en vue d'obtenir le consentement) par lequel il consent, ou ne consent pas au traitement des données qui le concernent. Il serait utile également, sans doute, afin de renforcer le caractère non équivoque du consentement d'inciter (ou de contraindre) les responsables de traitement à opter pour des systèmes d'*opt-in* plutôt que d' *opt-out*.

Outre l'exigence du consentement libre, spécifique, éclairé, non équivoque, les traitements de type Big Data semblent heurter de front les principes de minimisation des données et de finalité des traitements.

- *Minimisation des données (**article 5.4.c)***

Dans la mesure où, comme expliqué plus haut, l'utilité réelle d'une donnée – y compris une donnée à caractère personnel - dépend de la quantité des autres données récoltées avec lesquelles elle pourrait être agrégée, les responsables de traitement ont nécessairement tendance à les conserver non seulement lorsqu'elles sont utiles ou nécessaires à la fourniture d'un service déterminé, mais aussi en excès de ce qui serait strictement nécessaire aux services dont ils gratifient leur clientèle. Ainsi, alors que la géolocalisation continue des utilisateurs par les opérateurs de téléphonie mobile ne peut être justifiée en dehors des moments où l'utilisateur utiliserait spécifiquement certaines applications (la recommandation automatisée de restaurants à proximité de là où il se trouve par exemple) nécessitant la géolocalisation, il est de fait extrêmement difficile pour un utilisateur de s'assurer que ses données sont traitées conformément aux engagements spécifiques de l'opérateur et en conformité avec la législation en vigueur, car, bien sûr, rien de tout cela ne se voit ni ne s'éprouve.

Il conviendrait à cet égard de renforcer l'effectivité de l'obligation de déclaration des traitements de données (aux autorités de protection des données) ainsi que, comme déjà évoqué plus haut, l'obligation d'information des personnes concernées, y compris lorsque la finalité des traitements n'est pas autrement définie que de constituer des jeux de données suffisamment massifs que pour constituer la base de traitements de type *Big Data*.

Peut-être conviendrait-il également de soumettre à l'autorisation des autorités de protection des données la constitution de banques de données anonymisées aux fins de traitements de type *Big Data*.

- *Finalité (**article 5.4.b**)*[69]

De même, il est douteux que les utilisateurs de certains réseaux sociaux, en donnant leur consentement formel à la conservation et à l'exploitation de leurs données à des fins de recherche et d'amélioration des fonctionnalités du réseau aient réellement voulu donner la permission de se servir d'eux comme « cobayes » pour des expériences de psychologie sociale menées sur ce réseau et consistant à tenter de manipuler leurs émotions en triant, pendant un certain temps, le « fil d'actualités » auxquels ils étaient exposés de manière à étudier l'incidence, sur leur humeur, d'une exposition relativement prolongée à des expressions plutôt pessimistes, négatives, alarmistes, etc. C'est, cette fois, le principe de finalité qui se trouve mis à mal. Mais ce dernier est bien sûr également incompatible avec l'idéologie des *Big Data*, en cela soutenue par l'impératif de l'innovation érigé au rang de logique absolue et qui intime de ne pas brider la capacité des *Big Data* à faire émerger de nouveaux produits et services à la faveur, précisément, de la disponibilité de quantités massives de données dont la croissance ne serait bridée par aucun impératif de finalité.

1. Il semble qu'une réflexion devrait avoir lieu à propos de la distinction, qui semble s'estomper dans les esprits, entre liberté de la recherche scientifique et l'impératif d'innovation. Si nous n'entrerons pas ici dans cette discussion là, qui nous éloignerait trop des enjeux de la protection des données, constatons néanmoins que si la liberté de la recherche scientifique fait partie des valeurs prises en compte par la Convention 108 lorsqu'elle prévoit, à l'article 9 (dérogations et exemptions), la possibilité de restreindre les droits des personnes concernées dans le cas de traitements ne présentant aucun risque. L'exemple donné est celui de l'utilisation des données à des fins statistiques, dans la mesure où il s'agit de données présentées sous une forme agrégée et séparée des identifiants. De même la recherche scientifique est mentionnée dans cette rubrique. Il va de soi qu'il convient de distinguer les traitements de type *Big Data* des traitements de données à des fins statistiques. Nous avons expliqué plus haut en quoi les traitements de type *Big Data* consistent en de nouvelles pratiques statistiques différentes des pratiques statistiques classiques. Par ailleurs, la condition d'exemption des traitements statistiques est qu'elle ne « présente aucun risque » pour les individus (comme explicité dans le Rapport explicatif de la Convention 108). Or, dans le cas des traitements de type *Big Data*, les perspectives de profilage, y compris de profilage anticipatif, des personnes ainsi que les perspectives de décision automatique à l'égard des personnes (voir troisième partie *infra*) sont loin de ne poser aucun risque pour les personnes concernées. La « liberté d'innover », par contre, ne fait pas partie des valeurs implicitement ou explicitement protégées par la convention 108, ni des droits et libertés fondamentaux consacrés par la Convention européenne des droits de l'homme.
2. Il convient donc de réaffirmer très fermement le principe de finalité des traitements de données à caractère personnel, en l'étendant, le cas échéant, aux données anonymisées, conformément à ce que nous avons écrit plus haut à ce propos.

[69] A propos du principe de finalité, voir *l'Opinion 03/2013 on purpose limitation* du groupe de travail sur la protection des données de l'Article 29, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

- *Principe de loyauté et de transparence des traitements (**article 5.4.a)***

[On peut noter une éventuelle redondance entre les exigences de transparence prévues à l'article 5.4.a et à l'article 7bis de la Convention 108 révisée d'une part, et à l'article 5.2. d'autre part (concernant l'exigence d'un consentement libre, *spécifique*, *éclairé et non équivoque*, la quelle exigence emporte nécessairement, elle aussi, une exigence de transparence). Notre suggestion serait, à cet égard, de reformuler l'article 5.4.A comme suit: "a. traitées loyalement à l'égard de la personne concernée".]

Il conviendrait peut-être d'insister ici sur le fait que cette obligation de loyauté s'étend à l'ensemble des traitements de données, en ce compris la collecte (cf. *supra*), l'éventuelle anonymisation (auquel cas l'obligation de loyauté impliquerait notamment qu'il soit procédé à une évaluation des risques de réidentification et à une communication de cette évaluation à la personne concernée), …

- *Principe de limitation dans le temps (**article 5.4.e)***

En raison des risques de réidentification par croisement de données anonymes, la seule anonymisation ne devrait pas suffire à absoudre le responsable du traitement de toute obligation à l'égard des personnes concernées. En outre, le responsable de traitement devrait avoir notamment l'obligation de conformer les techniques d'anonymisation qu'il utilise à l'état de l'art en la matière. Dans la mesure où le risque de réidentification augmente avec le temps et les progrès des techniques de réidentification,[70] il convient de réaffirmer, peut-être d'avantage encore dans un contexte de données massives que dans d'autres contextes, le principe de limitation dans le temps, y compris, le cas échéant, pour les données anonymisées lorsque les techniques d'anonymisation ne garantissent pas contre le risque de réidentification.

2.3 Données sensibles (article 6)

Parmi les données qui nourrissent les traitements de type Big Data, les données sensibles (révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, les données relatives à la santé ou à la vie sexuelle, les données génétiques et biométriques, les données relatives à l'appartenance syndicale, les données concernant les condamnations pénales, les infractions et autres mesures de caractère pénal) par nature *ou qui le deviennent du fait de leur utilisation*[71] ne sont pas une catégorie minoritaire. Les images des personnes donnent des informations sur leur origine ethnique, le profilage des personnes sur base de leurs préférences en termes de cinéma et de divertissement (Netflix, télévision à la demande,…) est porteur d'indications relatives aux opinions politiques des personnes ou à leurs convictions religieuses, le relevé des habitudes de consommation dans les supermarchés peut également donner des indications relatives à l'état de santé actuel ou futur, ou aux pratiques religieuses des consommateurs.

Deloitte explique ainsi qu'il leur est possible, sur base de données de consommation dans les supermarchés, de déterminer l'état de santé actuel et futur d'une personne avec une précision comparable à un examen médical. Ces « profils de

[70] cf. l'Avis 05/2014 du groupe de travail de l'article 29 sur les techniques d'anonymisation: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

[71] Suivant la distinction introduite à l'Article 6 de la Convention 108 par le Comité as hoc sur la protection des données (3ème réunion, 1-3 décembre 2014).

consommateurs » suffiraient à détecter les propensions des individus à développer des maladies comme le diabète, cancer féminin, cancer corrélé à la consommation de tabac, maladie cardiovasculaire, dépression, etc.)[72] Alors que, classiquement, les candidats à l'assurance n'ont à déclarer à l'assureur que les conditions préexistantes, les maladies et handicaps dont ils se savaient atteints, la possibilité, pour les assureurs, de détecter des maladies ou des propensions à des maladies chez leurs clients sans même que ceux-ci aient connaissance de leur état induirait une asymétrie d'information très défavorable aux assurés.

Dans notre société hyper-connectée, d'après les calculs d'IBM, au cours d'une vie, un individu devrait produire plus d'un million de gigabytes de données sur sa santé. Ces données de santé ne sont plus seulement produites par le médecin, l'hôpital ou l'assurance-maladie, mais aussi par les individus eux-mêmes, qu'ils soient malades ou bien portants, au fur et à mesure que se répandent les gadgets connectés destinés à surveiller en permanence une série de marqueurs physiologiques (rythme cardiaque, poids calories brûlées quotidiennement, …). Les données relatives à l'alimentation, les données de fréquentation des clubs sportifs, les données de connexion à certains sites d'information ou de discussion à propos de la santé,… toutes ces données entrent potentiellement dans la catégorie des données relatives à la santé actuelle ou future. Si l'on ajoute à cela les données produites par séquençage de l'ADN humain, qui atteignent des volumes de dizaines de terabytes par génome, il semble que, dans les Big Data, les données de santé occupant une place importante. Au fur et à mesure que s'accumulent, grâce aux Big Data, des corrélations[73] nouvelles entre des éléments *a priori* sans liens avec la santé et le développement de certaines maladies ou la survenance de certains handicaps (modes de vie, habitudes alimentaires, éléments climatiques et environnementaux, …), le champ des données qui deviennent sensibles du fait de leur utilisation s'étend à des types de données que l'on n'aurait jamais pensé rattacher à la catégorie des données sensibles. Si une attention particulière doit être accordée aux données relatives à la santé, c'est qu'elles sont, parmi les *Big Data*, au nombre de celles qui "croissant" le plus vite, à la faveur notamment des nouveaux marchés, florissants, de la "santé connectée".

Par contre, un effet des approches de type *Big Data* notamment dans le domaine de la sécurité et de la prévention des fraudes, est que la valeur et l'utilité des données "visuelles" comme celles qui peuvent être révélatrices de l'origine ethnique, par exemple, décroit considérablement. La *visualisation* algorithmique des relations subtiles entre données, permet des découvertes inattendues et, à ce titre, nous émanciperait du joug de la représentation, du point-de-vue humain, toujours trop partiel et partial, toujours trop situé, empreint de préjugés, réfractaire à la nouveauté, au profit d'une "curiosité automatique" sans préjugés, capable d'ajuster en permanence ses modélisations aux nouvelles données qui l'abreuvent en continu.

Il importe ici, pour bien percevoir les enjeux, de distinguer clairement deux manières particulières de catégoriser les individus et/ou leurs comportements. Dans *les processus classiques de classification*, qui sont ceux qui étaient envisageables avant le tournant numérique et les nouvelles techniques d'analyse des données de type Big

[72] Aaron Rieke, David Robinson and Harlan Yu, *Civil Rights, Big Data and our Algorithmic Future*, A September 2014 report on social justice and technology, Upturn.

[73] "La corrélation, c'est ce qui quantifie la relation statistique entre deux valeurs (la corrélation est dite forte si une valeur a de fortes chances de changer quand l'autre valeur est modifiée, elle est dite faible dans le cas où une valeur a de faibles chances de changer quand l'autre valeur est modifiée" (Jean-Paul Karsenty, "Big Data (mégadonnées). Une introduction", *Revue du Mauss permanente*, 1er avril 2015)

Data, les catégories (statistiques, sociales, culturelles,…) préexistent aux opérations de catégorisation, lesquelles consistent à examiner des catégories préexistantes afin de déterminer quelles caractéristiques peuvent être utilisées pour identifier ou prédire l'appartenance au groupe, et à placer, en conséquence, les individus porteurs de ces caractéristiques dans la catégorie correspondante. Dans les processus de catégorisation, la réalité perçue se trouve donc subsumée dans des catégories préexistantes, suivant une logique déductive: les individus s'identifient ou se reconnaissent consciemment (il peut s'agir d'un groupe de parents d'élèves, par exemple, ou d'un groupe de personnes faisant partie d'une association quelconque, ou de personnes se reconnaissant comme faisant partie d'un groupe ethnique, d'un mouvement politique, d'une communauté religieuse, d'un mouvement gay/lesbien/queer, etc.) ou sont identifiés par autrui (comme dans le cas des recensements et des inscriptions dans des catégories statistiques), comme faisant partie d'un groupe en raison de certains attributs communs à tous les membres du groupe. Dans l'Union européenne, les directives anti-discrimination interdisent la discrimination lorsqu'elle est fondée sur l'appartenance d'une personne à l'une ou plusieurs des catégories qu'elles énumèrent : nationalité, sexe, origine ethnique, croyance religieuse, handicap, âge, orientation sexuelle. Ces « caractéristiques protégées » sont le fruit d'une prise de conscience de ce que les critères d'appartenance qui les définissent sont, plus que d'autres, de nature à exposer ceux qui en sont porteurs à des distinctions de traitement défavorables.

Les processus de regroupement ou clustering, consistent plutôt à faire surgir des catégories précédemment inconnues, socialement et visuellement imperceptibles, au départ de l'analyse de données, sans référence à aucune information préexistante concernant ces groupes ou catégories nouvelles. Dans les processus de regroupement ou clustering, les individus sont placés par autrui – cet *autrui* pouvant être un système de traitement automatisé de données - dans des « catégories » socialement, existentiellement insignifiantes et imperceptibles (puisqu'elles surgissent en cours de route) et ce, sans qu'ils puissent, le plus souvent, s'en rendre compte ni s'y reconnaître. Si l'on devait faire une typologie des « groupements » humains, une première distinction à faire serait donc, entre les catégories dans lesquels les individus se catégorisent eux-mêmes, ou peuvent à tout le moins se reconnaître, c'est-à-dire des groupes plus ou moins auto-organisés - dans lesquels peuvent exister des rapports de solidarité, de loyauté, d'interdépendance, ainsi que des opportunités de défense des intérêts du groupe - et les groupes dans lesquels les individus sont catégorisés par autrui et dans lesquels les individus, le plus souvent, ignorent faire partie de la « catégorie » en question. C'est tout le sens de la distinction à faire entre catégorisation et regroupement.[74] La catégorisation subsume la réalité perçue dans des catégories préétablies (sans les remettre en question), lesquelles sont les résultats de processus politiques, culturels, esthétiques, idéologiques,… c'est-à-dire toujours déjà d'une perception située et d'une interprétation du monde, alors que le regroupement, ou *clustering* apparaît comme le résultat automatique, « quasi naturel » du traitement statistique de « données » qui prennent l'allure de « faits ». Les régimes de protection contre la discrimination seront difficilement applicables aux distinctions de traitement faites sur base de ce type de regroupement ou *clustering*, puisque, par définition pourrait-on dire, ce n'est pas en raison de l'appartenance d'une personne à

[74] Bart Herman Maria Custers, *The Power of Knowledge. Ethical, Legal and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Tilburg: Wolf Legal Publishers, 2004.

telle ou telle catégorie protégée qu'on lui applique un traitement différent, mais en raison de modélisations imperceptibles.

L'avantage perçu des processus de regroupement sur les processus de catégorisation, c'est, donc, précisément, une certaine « innocence » (sociale, politique, idéologique), et le contournement des catégories inévitablement « biaisées » à travers lesquelles nous sommes, nous, les êtres humains, prédisposés à percevoir le monde. C'est d'ailleurs l'un des arguments fréquemment évoqué en faveur du remplacement des personnels de sécurité et des personnels de douane dans les aéroports par des dispositifs automatiques fondés sur un profilage informé par les Big Data. La cécité des traitements de type Big Data relativement aux catégorisations socialement éprouvées, et discriminantes, leur impartialité donc, serait, de l'avis de Tal Zarsky, l'une des mauvaises raisons pour lesquelles le *datamining* serait si mal perçu par la majorité, en raison de son "goût pour la discrimination": les individus relevant de « la majorité » préfèrent que la charge (en termes de coûts et d'inconvénients) des phénomènes de surveillance soit focalisée sur des groupes minoritaires spécifiques dépourvus de relais politiques plutôt que de subir eux aussi un système de surveillance qui y soumettrait tout le monde de manière égalitaire (sous une sorte de « voile d'ignorance »). Ce que promettraient les approches fondées sur les *Big Data* dès lors, ce serait une plus grande égalité, et la prévention des discriminations[75]. Ce n'est pas pour autant, comme nous le verrons plus loin, que les approches *Big Data* évitent les phénomènes de discrimination indirecte, voir les renforce dans la mesure où "les données" sont elles-mêmes le reflet assez fidèle des normativités sociales à l'œuvre dans le monde physique mais rendues "indétectables" dans la masse des données. (Nous aborderons la question de la discrimination indirecte plus loin).

La question que se pose, des lors, est celle-ci: l'approche consistant à énumérer une liste de catégories (et donc de données) sensibles est-elle la plus adéquate pour prévenir la discrimination dans un contexte où, d'une part, les éléments les plus triviaux de la vie quotidienne deviennent potentiellement des indicateurs de l'état de santé actuel ou future et d'autres caractéristiques sensibles de l'individu, et ou, d'autre part, les distinctions de traitement entre les personnes peuvent être réalisées de plus en plus finement, sur base non plus de leur appartenance à tel ou tel groupe historiquement discriminé, mais sur base d'éléments singuliers de leur mode de vie?

2.4 Sécurité des données (Article 7)

Les risques de « fuites » de données à caractère personnel résultant de failles de sécurité dans les systèmes de collecte, de stockage et de traitement de ces données, dans la mesure notamment où ils risquent d'affaiblir la confiance des individus dans l' « économie numérique » et, ainsi, de réduire d'autant les opportunités et revenus des entreprises, font l'objet d'investissements importants de la part des acteurs et régulateurs de l'économie numérique. Pour autant, la sécurisation des traitements de données est un défi particulièrement difficile à relever étant donnés l'éclatement de la propriété des données et leur distribution spatio-temporelle, la disparité des appareils connectés, la diversité des acteurs intéressés, la diversité des données, la généralisation des applications de Cloud computing, etc.

[75] Tal Zarsky, "Governmental Data Mining and its Alternatives", 2011, *Penn State Law Review*, Vol. 116, No. 2: "if data mining is accepted by the legislature, it might only require limited judicial review. This is as opposed to the use of profiles and field officer discretion, which calls for greater scrutiny."

Dans le contexte des Big Data, les risques de ré-identification des personnes concernées au départ de données anonymes ou anonymisées justifierait que l'obligation, pour le responsable du traitement, ainsi que, le cas, échéant, pour son sous-traitant, de prendre des mesures de sécurité appropriées (dont des mesures techniques de cryptographie, de contrôle et d'enregistrement d'accès, de sauvegardes automatiques,…) contre les risques tels que l'accès accidentel ou non autorisé aux données – y compris les données anonymes ou anonymisées – leur destruction, leur perte, leur modification ou leur divulgation.

Les autorités de contrôles (prévues à **l'article 12bis**) devraient être encouragées à coopérer entre elles (sous forme d'échange d'informations dans le cadre prévu à l'**article 12bis7.a**) pour l'établissement, la mise à jour, et la communication au public de recommandations en matière de sécurisation des traitements de données conformes à l'état de l'art. [76] Ainsi, l'**article 12bis 2.e.** pourrait-il être complété par l'ajout du point suivant: "(iv) de fournir aux responsables de traitement des recommandations conformes à l'état de l'art en matière de sécurisation des traitements de données. Pour ce faire, les autorités de contrôle sont encourages à échanger entre-elles toutes les informations pertinentes et utiles."

Cependant, on l'aura compris, les enjeux de la sécurisation des traitements ne sont pas spécifiques aux traitements de type Big Data. Dans l'univers des Big Data, le danger majeur, pour les droits et libertés fondamentaux, en ce compris les droits économiques et sociaux, provient moins d'éventuelles actions malintentionnées ou de négligences coupables (induisant notamment les failles de sécurité) que d'une nouvelle rationalité gouvernementale consistant à fonder la plupart des décisions sur la seule « intelligence des données ». La banalisation des traitements fondés sur la rationalité algorithmique, de bonne foi, dans les administrations publiques et dans les entreprises du secteur privé, ou le mariage de la bureaucratie bien intentionnée et des algorithmes sont porteurs d'enjeux beaucoup plus spécifiques et bien différents des enjeux liés aux brèches de sécurité.

2.5 Transparence des traitements (article 7bis)

Le texte révisé de la Convention 108 prévoit, à **l'article 7bis**, au titre du principe de la transparence du traitement de données, l'obligation, pour le responsable du traitement, d'**informer** les personnes concernées

de son identité et de sa résidence ou de son lieu d'établissement habituels,

de la base légale et des finalités du traitement envisagé

des catégories de données à caractère personnel

le cas échéant, des destinataires ou catégories de destinataires des données à caractère personnel et

[76] Voir çà cet égard, par exemple, les recommandations émises par la Commission belge pour la protection de la vie privée: http://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2013_0.pdf

des moyens d'exercer les droits énoncés à l'Article 8 [cf. infra], ainsi que de toute autre information complémentaire nécessaire pour garantir un traitement loyal et transparent des données à caractère personnel.

Il nous semblerait légitime, dans le contexte des Big Data, que le devoir d'information à l'égard des personnes concernées inclue les informations relatives à l'intention de réutilisation des données, même sous forme anonymisée, à des fins différentes des finalités explicitement déclarées au moment du recueil du consentement. De plus, comme évoqué plus haut, il pourrait être légitime d'étendre le devoir d'information aux risques (quantifiables) de réidentification des individus dans les situations impliquant le traitement de données anonymisées. Seule la connaissance de ces risques, en effet, permettrait de consentir en connaissance de cause.

Enfin, il semble légitime, afin d'éviter de trop grandes asymétries d'information ainsi que des distorsions de concurrence, que lorsque des traitements de type *Big Data* sont envisagés afin d'adapter les stratégies de marketing ou de faire varier des offres commerciales (variation des prix, de la qualité des produits, offres de « bonus »,…) en fonction des caractéristiques comportementales, de mode de vie, ou de toute autre caractéristique individuelle détectée grâce à des analyses de type *Big Data* ou au « tracking » de l'activité et des trajectoires des personnes, celles-ci en soient informées par une indication en marge, mais bien visible/perceptible, dans la communication marketing et au plus tard au moment de l'offre commerciale personnalisée.[77] L'indication de ces finalités libellées en termes d' « amélioration des services ou de l'expérience utilisateur » n'est souvent pas adéquate et induit le consommateur en erreur dès lors que la finalité est d'adapter l'offre ou les conditions commerciales à son « profil » (l'opération n'ayant souvent pas pour finalité de maximiser son utilité, son bien-être, mais bien de maximiser les profits de l'entreprise commerciale).

2.6 Droits des personnes concernées : décision fondée sur des traitements automatisés de données (article 8)

L'**article 8** prévoit notamment que

> Toute personne doit pouvoir:
>
> ne pas être soumise à une décision l'affectant de manière significative, qui serait prise sur le fondement d'un traitement automatisé de données, sans que son point-de-vue soit pris en compte;
>
> (…)
>
> obtenir, à sa demande, connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement lui sont appliqués

- *La force normative des dispositifs automatisés.*

[77] Executive Office of the President of the United States, *Big data and Differential Pricing*, Février 2015, https://www.whitehouse.gov/sites/default/files/docs/Big_Data_Report_Nonembargo_v2.pdf

La “force normative” du résultat du traitement de données (le caractère plus ou moins contraignant, persuasif, ou incitatif de la modélisation ou de la “prédiction comportementale” qui en résulte) dépend de plusieurs facteurs.

Des *facteurs propres à la finalité du dispositif*, en premier lieu: s’agit-il d’un dispositif d’aide à la décision, d’un dispositif de recommandation, ou d’un dispositif se substituant à la décision humaine? La force contraignante des résultats du traitement de données dépend bien entendu de la finalité (assistance informationnelle, recommandation ou décision) du système.

Des facteurs propres au fonctionnement « matériel » du dispositif : s’écarter de la recommandation est-elle seulement techniquement possible sans ralentir ou empêcher toute action ? Ainsi peut-on imaginer une voiture « intelligente » qui « refuserait » de démarrer tant que tous les passagers n’ont pas bouclé leur ceinture de sécurité. Ce type de dispositif est porteur d’une normativité « constitutive » : désobéir à l’injonction (boucler sa ceinture) équivaut à ne pas pouvoir du tout utiliser l’objet (la voiture). Autre exemple : la détection automatique de comportements suspects dans des aéroports qui, au lieu de « seulement » lancer une alerte à destination des personnels de sécurité, provoquerait l’arrêt immédiat de tous les ascenseurs, escalators, et la fermeture de toutes les portes des zones ouvertes au public. Ignorer l’alerte, dans ce cas, équivaut, pour les personnels concernés, à un blocage complet de l’aéroport. Le déclenchement du dispositif les contraint donc, quasiment matériellement, à intervenir, indépendamment de l’évaluation qu’ils auraient pu faire de la situation.

Mais, même dans le cas de systèmes ne se présentant que comme de simples systèmes de recommandation ne se substituant pas à la décision humaine, *des facteurs relatifs à l’organisation du travail, à l’évaluation de la productivité professionnelle bref, au contexte managérial* dans lequel intervient le processus décisionnel mais aussi des *facteurs relatifs à la psychologie de l’opérateur humain* ayant à suivre ou à s’écarter de la recommandation automatique (sa plus ou moins grande aversion au risque, son sens plus ou moins aiguisée de la responsabilité individuelle, ses prédispositions à se soumettre ou à résister aux injonctions d’accélération des processus décisionnels…) peuvent augmenter considérablement la force normative de la recommandation automatique, laquelle pourra être, dans certains (rares) cas, ignorée ou au contraire (vraisemblablement dans la plupart des cas) quasi automatiquement et intégralement transposée dans la décision de l’opérateur humain. Ainsi peut-on imaginer qu’il soit difficile, dans un certain nombre de cas, à l’agent humain de s’écarter de la recommandation automatique, dans la mesure où cet écart, d’une part, risquerait de faire baisser son niveau de productivité, et, d’autre part, le contraindrait à assumer personnellement la décision et ses conséquences, et à s’en justifier en cas de conséquence défavorable, alors qu’une décision conforme à la recommandation lui eût permis de reporter la responsabilité sur le système informatique. La seule existence d’une recommandation automatisée induit aussi, pour celui qui voudrait s’en écarter, le devoir de justifier son écart non pas tant « en son âme et conscience », ou en fonction, par exemple, d’une certaine idée qu’il se ferait de l’équité ou de la justice, eût égard à la situation concrète dans laquelle il a eu à décider, mais en fonction d’arguments au moins aussi quantifiables que le sont les prédictions algorithmiques. On le voit, ce qui disparaît ici, c’est la notion même d’indécidabilité, d’incertitude radicale, celle-là même qui oblige les juges à « trancher » alors même qu’ils savent que la justice n’est jamais qu’un idéal régulateur, inatteignable par la seule voie du calcul. Ce qui disparaît également, ce sont les occasions, pour les opérateurs humains, de diverger de la décision ‘optimale’ en raison d’une incitation – incalculable et imprévisible – à la clémence, à la générosité ou à la solidarité, toujours injustifiables par les seuls arguments quantitatifs. Enfin, ce qui

risque, à terme, de s'émousser, à force de n'être pas utilisée, c'est la capacité individuelle des opérateurs humains à évaluer par eux-mêmes les cas et situations qui leur sont présentés. Cette nouvelle forme de « prolétarisation »[78] - de perte de capacités – engendrée par les systèmes automatisés d'aide à la décision – rend les opérateurs humains intimement dépendants de leurs appareils, au risque – en cas de défaillance technique – de les rendre incapables de ne prendre aucune décision.

- *Décision automatisée et justiciabilité des décisions. Que mettre en procès : les faits ou les conditions des faits ?*

Si l'on prend acte de tout cela comme d'un état de fait, et si l'on veut aussi y voir non pas tant un danger mais un progrès (accélération et objectivation des processus décisionnels, évitement des bais, préjugés, erreurs d'évaluation toujours possibles dans le traitement humain des situations, diminution des coûts en personnel de sécurité dans les lieux massivement ouverts au public,…), on sera tentés de ne percevoir les risques potentiels pour les droits et libertés fondamentaux qu'en termes d'erreurs éventuelles des machines, erreurs causées soit par le caractère erroné ou incomplet des données traitées (mais l'hypothèse fondamentale – mais en partie idéologique - des Big Data est qu'elles tendent à l'exhaustivité, cf. p. 12), soit par l'inadéquation de la modélisation (comme des erreurs d'assomption, cf. p.14), erreur des machines qui présuppose qu'existe, par ailleurs, une « vérité objective » - vérité équivalente aux faits eux-mêmes - laquelle eût été trouvée *nécessairement*, n'était-ce l'occurrence de/des erreurs (dont on postule aussi qu'elles sont détectable et corrigibles, ce qui, nous l'avons vu (p.14), est loin d'être évident. L'argumentation présume une adéquation totale entre les faits perceptibles à travers leur transcription numérique et la justice, qui n'en serait que la transposition décisionnelle. C'est, bien entendu, oublier que comme l'écrivait Georges Canguilhem que « le fait n'a point par lui-même de valeur. Et même, du moment qu'il existe comme fait, c'est qu'il porte avec lui ses conditions. Les conditions, qui les connaît les change. Aussi le fait traduit-il non pas ce qu'on fait mais ce qu'on ne fait pas. » [79] La renonciation à comprendre les causes des phénomènes au profit de la recherche de prédictions sur une base purement statistique, inductive, ou, autrement dit, l'indifférence pour les causes des phénomènes c'est aussi la renonciation à connaître et à changer *les conditions des faits*.

Si la rationalité algorithmique dispense de s'interroger sur les raisons pour lesquelles, par exemple, dans les bases de données obtenues auprès des employeurs d'une région, on retrouve, parmi les employés exclus prématurément de la force de travail, ou n'ayant pas obtenu d'avancement, d'avantage de personnes désignées comme appartenant à un certain groupe ethnique déterminé, ou de personnes de sexe féminin,…la cause (les tendances discriminatoires dans la société), devient *imperceptible* alors que se construisent sur cette base des « profils » d'employabilité accaparant le statut de « fait objectif » : la déduction pratique, ou la recommandation automatisée à destination des gestionnaires de ressources humaines sera celle-ci : « les personnes appartenant à certains groupes ethniques ou de sexe féminin sont, statistiquement, professionnellement moins performantes », sans que les discriminations (qui ne sont pas toujours nécessairement officiellement identifiés comme telle car tout le monde ne va pas en justice pour faire reconnaître une

[78] Voir, à propos de ce concept de prolétarisation voir notamment Bernard Stiegler, *La société automatique*, *1. L'avenir du travail*, Fayard, 2015, p. 43.
[79] Georges Canguilhem, « La mobilisation des intellectuels : protestations d'étudiants », *Libres propos*, 20 avril 1927, p.54.

discrimination illégale), qui sont les *conditions de ce « fait »*, soient encore perceptibles comme problématiques.

On le voit ici de façon exemplaire, et nous l'avons déjà évoqué précédemment : les analyses de type *Big Data* prétendent à une certaine forme d'objectivité[80]: non pas une objectivité *critique* qui s'appuierait sur la connaissance des circonstances, du contexte, des causes des phénomènes, et donc sur une prise en compte de leur contingence, mais une objectivité *machinique* qui s'appuie d'une part sur l'automatisation des processus de traitement de données et la mise à l'écart de la subjectivité (sélectivité, point-de-vue situé[81], représentation, interprétation) et, d'autre part, sur l'apparente indépendance des modélisations algorithmiques relativement aux catégorisations politiquement instituées et socialement éprouvées.

Pourtant, les algorithmes, même, et peut-être surtout lorsqu'ils deviennent "auto apprenants", incorporent certaines « visions du monde », notamment les visions du monde tolérantes à la discrimination, et permettent en outre d'opérer des distinctions de traitement, dans le contexte de l'emploi, en fonction d'éléments ou de critères très peu transparents (aux yeux même de ceux qui utilisent les algorithmes à des fins de sélection) et en eux-mêmes, individuellement, sans rapport avec les exigences de la fonction ou du poste de travail. Mais l'opacité des processus algorithmiques, leur « couverture » par le secret industriel, rendent les discriminations éventuelles très malaisées à prouver, d'autant que, la plupart du temps, l'intention discriminatoire n'est pas du tout présente dans le chef de la personne qui utilise ces dispositifs automatiques afin d'objectiver ses propres décisions. La discrimination indirecte résultant de l'intervention du système de recommandation automatisé n'est pas tant dû à la personne qui déciderait de suivre la recommandation (au contraire, pourrait-on dire : le fait pour elle de vouloir objectiver de la sorte les décisions peuvent attester de sa volonté de neutraliser ses propres préjugés) qu'à la préexistence, dans la société, d'un *animus* discriminatoire (un « goût » ou une tolérance pour la discrimination) plus ou moins répandu, lequel se reflète passivement dans les jeux de données et acquiert par là même le statut de fait objectif, apolitique, neutre, non problématique.

Une solution dès lors serait peut-être d'exiger bien d'avantage que la seule possibilité, pour la personne concernée par une décision l'affectant significativement et prise sur le fondement d'un traitement automatisé de données, de faire valoir son point-de-vue. Tout peut laisser penser que ce point-de-vue sera de peu de poids au regard de l'objectivation algorithmique attendue des systèmes automatiques. Par ailleurs, et plus en amont dans le processus, l'influence qu'un individu peut avoir sur le profilage est très limité : les modélisations prédictives ou profils supra-individuels qui lui sont assignés sont construits à partir de données infra-individuelles émanant de nombreux individus ; dans ce processus les données de n'importe qui sont aussi bonnes que celles de n'importe quel autre individu – *your data is as good as your neighbours* – ce

[80] Une objectivité qui tient à la relative non-sélectivité du rapport aux données numériques, à l'indépendance des modélisations algorithmiques relativement aux catégorisations socialement instituées et éprouvées, et à la minimisation de l'intervention humaine au profit des processus automatiques.

[81] Cependant les modélisations algorithmiques ne prennent en compte que ce qui est numérisé ou numérisable, indépendamment du fait que la numérisation soit toujours une transcription, et qu'il n'existe pas de transcription neutre du monde et de ses événements (ce qui est « capté » dépend toujours de la localisation, de la distribution, de la sensibilité des capteurs). Les « données brutes » elles-mêmes sont le résultat d'un travail sophistiqué de désindexation, de décontextualisation, de suppression de tout ce qui pouvait relier la donnée à ce qui fait la singularité d'une vie.

qui fait que très peu de données suffisent pour inférer un savoir nouveau. Toute l'information statistique pertinente à propos d'un individu se trouve déjà incluse dans le modèle avant même que celui-ci ait pu soumettre lui-même quelque information à propos de lui-même : les « personnes » sont oubliées littéralement oubliées dans le modèle.

En plus d'exiger une possibilité pour la personne concernée de faire valoir son point-de-vue, il s'agirait surtout d'exiger que toute décision affectant une personne de manière significative et prise sur le fondement d'un traitement automatisé de données soit dûment motivée au regard de la situation singulière de la personne concernée. En particulier, en cas de suspicion de discrimination indirecte résultant de l'implication, dans le processus décisionnel, d'un traitement automatisé de données, et en raison de l'opacité flagrante – et difficile à vaincre - des logiques de traitement impliqués (y compris lorsqu'interviennent des dispositifs auto-apprenants ou de machine learning), il conviendrait de mettre à charge de celui qui s'aide des dispositifs automatiques pour prendre la décision, la preuve de l'absence d'effets discriminatoires. Cette inversion de la charge de la preuve est tout à fait dans la ligne de l'obligations mise à charge du responsable de traitement par l'**article 8bis2**, de concevoir le traitement de données de manière à prévenir ou à minimiser les risques d'atteinte aux droits et libertés fondamentaux.[82]

Cette solution se heurte pourtant aux incertitudes subsistantes quant à l'applicabilité aux relations entre particuliers de l'Article 14 de la Convention européenne des droits de l'homme interdisant la discrimination fondée notamment sur le sexe, la race, la couleur, la langue, la religion, les opinions politiques ou toutes autres opinions, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance ou toute autre situation. Si aucun obstacle théorique ne s'oppose à la reconnaissance d'un effet horizontal de l'article 14 de la Convention[83] la possibilité d'engager la responsabilité des Etats en raison de leurs abstentions lorsque celles-ci ne permettent pas d'éviter des cas de discriminations entre personnes privées reste tributaire de l'interprétation de la Cour de Strasbourg.

Si cette incertitude pouvait être levée, il conviendrait alors

- de remplacer le texte de l'article 8 c par le texte suivant: "c. obtenir, à sa demande, connaissance de la justification, au regard de sa situation singulière, de la décision prise sur le fondement d'un traitement automatisé de données."
- D'ajouter, à la suite du texte de l'article 8bis2, la phrase suivante: "En particulier, chaque Partie prévoit que les responsables du traitement et les destinataires démontrent à l'autorité de contrôle compétente que les décisions prises sur le fondement de traitements automatisés de données ne produisent pas d'effets discriminatoires incompatibles avec le droit à l'égalité d'opportunités tel qu'il se déduit de l'Article 14 de la Convention européenne des droits de l'Homme.

[82] L'article 14 de la Convention européenne des droits de l'Homme stimule explicitement que "la jouissance des droits et libertés reconnus dans la présente Convention doit être assurée, sans distinction aucune, fondée notamment sur le sexe, la race, la couleur, la langue, la religion, les opinions politiques ou toutes autres opinions, l'origine nationale ou sociale, l'appartenance à une minorité nationale, la fortune, la naissance ou toute autre situation."

[83] Voir à cet égard Caroline Picheral, "Discrimination raciale et Convention européenne des Droits de l'Homme (l'apport de la jurisprudence), *Rev. trim. dr. h.* , 2001, pp. 517-539.

- *« Toute personne doit pouvoir obtenir, à sa demande, connaissance du raisonnement qui sous-tend le traitement de données, lorsque les résultats de ce traitement lui sont appliqués »* (**article 8.c**)

Dans le contexte de décisions prises sur le fondement d'un traitement de données de type Big Data, et, *a fortiori* lorsque celui-ci implique des algorithmes auto-apprenants (cf. supra, p.14), l'exigence de communication, à la personne concernée, du "raisonnement qui sous-tend le traitement de données" est à la fois peu réaliste et fondamentalement paradoxale.

Elle est peu réaliste dans la mesure où, par définition pourrait-on dire, les algorithmes (c'est surtout vrai en ce qui concerne les algorithmes auto-apprenants) fonctionnent sur des logiques inductives qui, se passant de "théories" ou d'hypothèses, ne sont pas aisément communicables aux êtres humains ni intelligibles pour eux. Ces logiques - ne sont pas facilement traduisibles sous forme narrative. Elles ne sont peut-être même pas, dans le cas des algorithmes non supervisés, tant des "logiques" que des "visions" de l'algorithme qui "repère", en fonction notamment d'impératifs d'optimisation de son propre fonctionnement, des modèles ou "patterns" au sein de masses de données relativement peu structurées. Et ce que "voient" les algorithmes ne nous est pas perceptible. Nous pouvons en ressentir les effets lorsque des décisions sont prises sur le fondement de la "vision algorithmique" mais ne pouvons expliquer le processus président au repérage, par l'algorithme, des corrélations susceptibles de se constituer en modèle.

Cette exigence de communication du « raisonnement qui sous-tend le traitement des données » est aussi paradoxale dans la mesure où comme l'explique David Golumbia, "des processus et des objets 'perçoivent' continuellement, de manière computationnelle, mécanique, informatique, physique, sans référence à nous et suivant des modalités que nous ne pouvons ni voir, ni enregistrer ni forcément comprendre. Exiger que nous soyons capables de voir quelque chose qui est à la fois invisible et sans relation avec les êtres humains et la perception humaine est clairement un paradoxe qui demanderait que *a* et *non-a* fussent vrais en même temps." [84]

Si l'exigence de la communication du « raisonnement »[85] sous-tendant le traitement de données lorsque les résultats de ce traitement sont appliqués dans le cadre d'une décision prise à l'égard d'une personne est effectivement de nature à améliorer la situation de la personne concernée en assurant à tout le moins une symétrie informationnelle entre elle et le responsable du traitement ou le destinataire, cette exigence est peu réaliste et invinciblement paradoxale dans le contexte des Big Data.

Enfin, même s'il était possible de communiquer aux personnes concernées les « raisonnements sous-tendant les traitements de données, cela ne serait pas du tout suffisant, à défaut de rendre également transparentes et communicables l'origine et la

---

[84] David Golumbia, "Judging like a Machine", in. David M. Berry, Michael Dieter (eds.), *Postdigital Aesthetics: Art, Computation and Design*, Palgrave Macmillan, 2015: "(…) computational, mechanical, informatic, physical 'perception' of processes and objects takes place at all time, without reference to us and in modalities we cannot see, register or necessarily understand. Demanding that we be able to see something that is at the same time invisible to and unrelated to human being and human perception is a clear paradox that demands both *a* and *not-a* be true at once."

[85] D'ailleurs, il n'est pas certain que ces processus algorithmiques, dès lors qu'ils deviennent auto-apprenants, soient encore assimilables à des « raisonnements », si par « raisonnement » on implique une dimension de jugement synthétique a postériori.

nature des données traitées, les caractéristiques des instruments d'enregistrement ou capteurs de ces données, les processus de « nettoyage » de ces données, alors même qu'une des caractéristiques des données massives est d'être *amnésiques* de leur contexte d'origine et des conditions matérielles de leur production.

Dans ce contexte, d'avantage que la transparence hors d'atteinte des logiques de traitement, c'est l'exigence d'une motivation de la décision au regard de la situation singulière (irréductible au « profil » produit par l'algorithme) de la personne concernée (cf.p. 40) qui nous paraît constituer une garantie importante contre l'algorithmisation excessive des processus décisionnels. Cette exigence de motivation singulière assure la contestabilité des décisions et évite la déresponsabilisation des acteurs humains qui les assument.

3. CONCLUSIONS.

DE NOS JOURS, CE SONT, DE MANIERE DE PLUS EN PLUS PREPONDERANTE, LES DONNEES NUMERIQUES QUI INFORMENT ET GUIDENT L'ACTION, DANS LA QUASI-TOTALITE DES SECTEURS D'ACTIVITE ET DE GOUVERNEMENT. LES DONNEES, PERSONNELLES OU ANONYMES SONT LES NOUVELLES COORDONNEES DE MODELISATION DU SOCIAL. C'EST A PARTIR D'ELLES, PLUTOT QU'A PARTIR DE PROCESSUS INSTITUTIONNELS OU DELIBERATIFS, QUE SE CONSTRUISENT LES CATEGORIES A TRAVERS LESQUELLES LES INDIVIDUS SONT CLASSES, EVALUES, RECOMPENSES OU SANCTIONNES, OU A TRAVERS LESQUELLES S'EVALUENT LES MERITES ET LES BESOINS DES PERSONNES OU ENCORE LES OPPORTUNITES OU LA DANGEROSITE QUE RECELENT LES DIVERSES FORMES DE VIE QU'ELLES HABITENT. DANS CETTE PERSPECTIVE D'UN « GOUVERNEMENT PAR LES DONNEES », COMMENT GARANTIR LA SURVIVANCE DES SUJETS DE DROIT ? COMMENT FAIRE EN SORTE QUE LES PERSONNES NE SOIENT PAS PRISES EN COMPTE SEULEMENT EN TANT QU'AGREGATS TEMPORAIRES DE DONNEES NUMERIQUES EXPLOITABLES EN MASSE A L'ECHELLE INDUSTRIELLE MAIS COMME DES SUJETS DE DROIT A PART ENTIERE ?

Les processus de personnalisation et de profilage (au détriment des approches « par catégories préexistantes ») propres à la gouvernementalité dans le monde des Big Data la distingue foncièrement des hypothèses décrites par Michel Foucault du « biopouvoir » - un pouvoir qui « s'exerce positivement sur la vie, qui entreprend de la gérer, de la majorer, de la multiplier »[86], « dont le rôle majeur est d'assurer, de soutenir, de renforcer, de multiplier la vie »[87] - , et de la « biopolitique de populations » - qui aurait émergé à partir de la seconde moitié du XVIII[ème] siècle visant les multiplicités humaines comme « une masse globale, affectée de processus d'ensemble qui sont propres à la vie et qui sont des processus comme la naissance, la mort, la production, la maladie »[88]-, biopouvoir et biopolitique avec lesquelles, bien

[86] Michel Foucault, *Histoire de la sexualité, t. I, La volonté de savoir*, Gallimard, 1976.
[87] *Ibid.*
[88] Michel Foucault, "*Il faut défendre la société". Cours au Collège de France, 1975-1976*, Gallimard/Le Seuil, "Hautes Etudes", 1997.

évidemment, le « gouvernement par les données » partage certain traits par ailleurs, dont le fait de reposer de manière cruciale sur des pratiques statistiques. Mais le terrain de la vie – celle des individus en tant que corps et psychismes individuels, et celle des populations en tant qu'affectées de processus d'ensemble propres à la vie - paraît singulièrement déserté au profit d'un terrain numérique de plus en plus refermé sur lui-même : comme si ce qu'il s'agissait aujourd'hui de « gouverner », ce n'était plus tant les individus en chair et en os, capables de pâtir et interpellés *en tant qu'ils seraient sujets de droits et d'obligations*, en tant qu'ils auraient à rendre compte de leurs actes et de leurs décisions, que des réseaux de données agrégées sous forme de modèles « prédictifs », n'incarnant rien d'autre que la pure potentialité, l'opportunité économique détectée en temps réel, c'est-à-dire de l'opportunité pure, non finalisée autrement qu'en termes d'accélération et d'objectivation des processus de décision eux-mêmes, c'est-à-dire, à terme, d'automatisation de la décision.

Fragmenté comme il l'est sous forme d'une myriade de données le reliant à une multitude de profils (de consommateur, de fraudeur potentiel, d'employé plus ou moins fiable, plus ou moins productif,…) qui, tous, ne se rapportent qu'à lui sans l'inscrire dans aucun contexte collectif (à la différence des modes « classiques » de catégorisations, comme le profilage ethnique, ajustés sur des catégorisations socialement éprouvées et donc susceptibles de donner lieu à des actions collectives), l'individu, dispensé d'avoir encore à rendre compte de lui-même, devient infiniment calculable, comparable, indexable, interchangeable, mis en concurrence – une concurrence *absolue*, qui n'est plus même bornée par, ni articulée à aucune norme (de mérite, de désirabilité, de besoin, d'équité…) - avec tous les autres à l'échelle quasi-moléculaire dans une économie de la réputation, du risque et de l'opportunité (plutôt que du projet) opérant de manière automatisée à l'échelle subliminale de la donnée infra-personnelle. Nous aimons à nous penser, individus du XXI^{ème} siècle, comme des processus en constante évolution, non clôturés, peu définis, pour les possibilités de nouveautés que cette absence de définition ménage plutôt que comme des êtres finis, achevés, définitivement rangés dans un statut social, une profession, une catégorie – raison pour laquelle nous tenons à garantir juridiquement, à travers le droit à la protection de la vie privée notamment, une « forme d'immunité contre les contraintes déraisonnables dans la construction de sa propre identité ». 89 Mais nous voulons aussi nous prémunir de « l'horreur de n'avoir ni ombre ni reflet, d'être réduit à une existence absolument blanche, mate, devenue poreuse et comme vidée de sa substance (…) l'épouvante d'être allégé de mon poids d'ombre intérieure, de cette douce fourrure trouble qui me double au-dedans et au-dehors de moi-même."90 Clément Rosset faisait remarquer qu'en français, « une personne, un certain homme, c'est aussi bien "personne" aucun homme: écho du lien originel qui soude le déterminé au non-déterminé, le quelque chose au n'importe quoi, la présence de mille chemins à l'absence de tout chemin."91 Cette double face du mot « personne » trahit une ambivalence motrice, au cœur même de la

---

[89] Philip E. Agre, Marc Rotenberg (eds.), *Technology and Privacy. The New Landscape*, MIT Press, 1998, p. 3. : ". . . control over personal information is control over an aspect of the identity one projects to the world, and the right to privacy is the freedom from unreasonable constraints on the construction of one's own identity."

[90] Michel Foucault, *L'usage de la parole: deuxième série: langages de la folie*: 4 - Le corps et ses doubles, 28 janvier 1963.

[91] Clément Rosset, *Le Réel. Traité de l'idiotie*, Minuit, 1977/2004, pp.18-19.

subjectivité, au principe même des processus de subjectivation : présence en devenir, la « personne » est inclôturable. Dans l'univers de données massives, à travers la télé-objectivité des profilages "prédictifs", c'est dans leur double dimension de présence et d'absence, dans leur paradoxe ou leur pli92 constitutif que les personnes se trouvent escamotées.

Les régimes juridique de protection des personnes à l'égard des traitements automatisés de données ont donc, en premier lieu peut-être pour tâche de garantir aux personnes, aux sujets de droit, à la fois une certaine présence, un poids, une consistance, dans un univers où seuls comptent des agrégats temporaires de données métabolisables en masse à l'échelle industrielle d'une part, et, d'autre part, d'empêcher l'enfermement des personnes dans des « catégories », des « profils », des « personnalisations » qu'ils n'auraient l'occasion ni de connaître, ni de contester. Donner consistance au sujet de droit, ce n'est pas "mettre le consommateur au centre" en l'entourant de dispositifs capables de détecter avant qu'il ne les ait lui-même réfléchies et énoncées ses éventuelles propensions d'achat, ce n'est pas non plus tenir, "préemptivement" pour actuelles les conduites n'existant sur le mode de la potentialité (dont la potentialité n'est avérée par rien d'autre que des modélisations algorithmiques), mais bien plutôt tenir compte, toujours, de la capacité qu'ont les personnes de ne pas faire de ne pas vouloir tout ce qu'elles sont « statistiquement » prédisposées à faire ou à vouloir, et de faire prévaloir, toujours, leur droit de rendre compte par elles-mêmes de leurs motivations. On ne respecte pas le sujet si on ne respecte pas à la fois sa capacité de réticence, de réserve, de non-effectuation de ce que les algorithmes prédisent à son propos, et sa capacité d'énoncer, par lui-même, ce qui le fait agir.

C'est à une revalorisation et à la protection par le droit de ces deux « facettes» essentielles du sujet de droit qu'invitent, en filigrane, les considérations qui précèdent. Ce qu'il convient dès-lors de garantir, à titre de « méta-droits », ou de capacités nécessairement reconnues et protégées dans un état de droit, c'est [93]

1) la faculté de désobéir, de n'être pas toujours déjà là où nous sommes attendus, de ne pas faire tout ce dont nous sommes capables d'après les projections algorithmiques ;

2) la responsabilité de rendre compte par nous-même de nos actes, décisions et intentions malgré les recommandations et profilages algorithmiques.

C'est donc à repenser, et à protéger par le droit, le centre de gravité de la subjectivité juridique qu'invitent les développements qui précèdent : non plus tant les capacités d'entendement et de volonté ni la maîtrise des intentions, mais une certaine propension à la spontanéité, à l'imprévisibilité, une ouverture à l'événement d'une part, et une capacité d'énonciation, fût-elle fabulatrice, d'autre part. Ce n'est qu'au prix de cette reconceptualisation du sujet de droit que l'on pourra imaginer le développement

[92] Nous renvoyons bien sûr au pli deleuzien (Gilles Deleuze, *Le pli. Leibniz et le baroque*, Minuit, 1988).

[93] Sur la notion de "méta-droit" – par laquelle nous entendons une série de capacités ou prérogatives individuelles nécessairement présupposées par l'état de droit et qui rendent possible la débatabilité et la contestabilité des normes, nous nous permettons de renvoyer le lecteur à Antoinette Rouvroy et Thomas Berns, « Le nouveau pouvoir statistique » Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps numériques », *Multitudes*, 2010/1 n° 40, p. 88-103.

harmonieux des applications fondées sur l'intelligence des données et des êtres politiques et solidaires que nous sommes. Pour le surplus, et par définition pourrait-on dire, nous n'aurons jamais fait le tour des Big Data et des enjeux éthiques, juridiques et politiques qu'implique le tournant numérique. Aussi est-ce à une vigilance constante et à un examen continuellement renouvelé de la pertinence et de l'adéquation des instruments juridiques de protection des droits et libertés fondamentaux qu'invite la « révolution numérique ».