

Université Paris V Descartes  
L3 Option Economie Quantitative  
2018/2019

Projet Tutoré

**ECONOMIE DES DONNEES  
PERSONNELLES**

Ayoub Barrou  
Mohamed Amara

## Sommaire

|                                                                                                                            |    |
|----------------------------------------------------------------------------------------------------------------------------|----|
| INTRODUCTION .....                                                                                                         | 3  |
| AXE 1 : Collecte et Mode de Production Des Données Personnelles.....                                                       | 5  |
| I. Les Différents Types de Données Personnelles .....                                                                      | 5  |
| II. Les Stratégies de Collecte des Données Personnelles .....                                                              | 7  |
| III. Les Modes De Production et Entreprises Concernées.....                                                                | 10 |
| AXE 2 : Stratégies d'exploitation, Externalités et Dilemmes du Consommateur .....                                          | 13 |
| I. Les Stratégies des Entreprises : Discrimination des prix et Personnalisation/Publicité<br>Ciblée et Marketing .....     | 13 |
| II. Les Externalités des Données Personnelles : .....                                                                      | 17 |
| III. Le Dilemme du Consommateur .....                                                                                      | 20 |
| AXE 3 : Protection des Données et ses Effets Face Au Marché .....                                                          | 24 |
| I. La Confidentialité/Traitement des Données Personnelles : Contraintes et Limites<br>Juridiques pour les Entreprises..... | 24 |
| II. L'Innovation et La Conformité à la Loi .....                                                                           | 29 |
| III. La Protection des Données dans le cadre de l'Union Européenne .....                                                   | 32 |
| CONCLUSION .....                                                                                                           | 36 |
| BIBLIOGRAPHIE ET WEBOGRAPHIE .....                                                                                         | 37 |

# INTRODUCTION

Chaque minute, l'humanité produit 350 000 Tweets, 15 millions de SMS, 200 millions de mails, 250 giga-octets d'informations sont archivés sur Facebook et 1 740 000 giga-octets d'informations sont publiés dans le monde. Tous les jours, Google traite plus de 24 pétaoctets de données, soit 24 millions de milliards d'octets. En 2013, 1,01 milliards d'objets connectés peuplent la planète. En 2020, nous estimons qu'il y en aura près de 100 milliards.

La notion des données personnelles est très vaste dans la mesure où elle s'étend à tout ce qui concerne une personne, c'est donc toute information relative à une personne physique pas forcément désignée. La donnée est au cœur des priorités stratégiques de plusieurs entreprises. L'information est partout et ses sources sont multiples, elle circule, se reproduit, se stocke et s'exploite. Une donnée à caractère personnel est relative à une personne physique qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. Mais il faut savoir que de multiples débats s'opposent sur la manière d'exploiter ces données personnelles et les stratégies utilisées pour les collecter qui peuvent nuire sur le bien-être et la vie privée des personnes concernées.

Le règlement européen RGPD est un règlement général sur la protection des données qui constitue le texte de référence en matière de protection des données à caractère personnel, Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne, ce règlement a été adapté en droit interne par la loi du 20 juin 2018 relative à la protection des données personnelles dont on donnera les détails plus loin dans notre exposé. Par ailleurs, cette loi donne à la CNIL (Commission Nationale de l'Informatique et des Libertés) des missions supplémentaires et un pouvoir de contrôle et de sanction accru en matière de protection des données. Internet, les technologies de l'information et de la communication ont permis de réduire considérablement les coûts de collecte et de traitement des données, ce sont de véritables accélérateurs de business.

Ces données individuelles qu'elles soient anonymes ou personnelles, représentent des enjeux sociaux mais surtout économiques importants car elles sont à la source de nombreux services. Quels sont alors ces enjeux-là, de quelle manière les entreprises exploitent ces données personnelles dans l'essor de leurs activités économiques et dans quelle mesure cela impacterait le bien-être des consommateurs ?

Afin de bien mettre en perspective tous les enjeux et impacts de la vie privée sur les entreprises ainsi que les individus, il nous apparaît nécessaire de procéder en trois étapes.

Nous allons sans doute présenter un état des lieux des définitions afin de mieux comprendre les concepts nécessaires à notre étude qui portera, dans un premier temps, sur le mode de production des données personnelles ainsi que les stratégies utilisées pour leur collecte et exploitation. Dans un second temps, nous allons aborder les conséquences économiques de l'exploitation de ces données c'est à dire les externalités positives et négatives de celles-ci en parlant du paradoxe comportemental consistant à ne pas se protéger contre les intrusions malgré une conscience des risques, mais à dévoiler sa vie contre une récompense. Et enfin nous finirons par le côté juridique, soit la participation de la protection des données et ces effets face au marché.

## AXE 1 : Collecte et Mode de Production Des Données Personnelles

Dans ce chapitre, nous allons entamer notre étude par une description des données personnelles, en évoquant ses différents types et statuts. Les différentes stratégies de collecte seront également couvertes dans ce premier axe ainsi que les différents modèles d'affaire des entreprises autour des données personnelles.

### **I. Les Différents Types de Données Personnelles**

Le web est devenu un moyen privilégié pour obtenir des données sur son marché et ses prospects. Ces données sont très précieuses pour les entreprises car elles leur permettent d'améliorer leur offre et leur marketing, afin de répondre plus précisément aux besoins de leurs cibles. Les individus émettent, intentionnellement ou non, d'innombrables informations les concernant, eux ou leurs proches, que ce soient leurs caractéristiques objectives, subjectives ou comportementales. Ces données, une fois collectées et traitées, permettent potentiellement d'identifier et profiler des personnes, de relier certaines de leurs caractéristiques individuelles à une donnée d'identification ou de contact, d'interagir avec elles selon des modes plus ou moins individualisés.

#### **1. Description des Données Personnelles**

Nous pouvons distinguer deux types de données :

D'un côté, il y'a ce qu'on appelle les données personnelles identifiantes : peuvent être sous catégorisées comme les données d'identification et de contact comme l'identité civile, l'adresse postale, numéro de téléphone, numéro d'immatriculation d'un véhicule, adresse électronique. Une autre sous-catégorie : données physiques de signalement telles que la taille, le poids, couleur de peau des yeux des cheveux, l'état de santé, maladie etc..... Les données sociodémographiques : l'âge, le genre, la date de naissance, le niveau ou même la profession.

Nous retrouvons aussi les données juridiques comme le casier juridique et enfin les données financières et foncières (solde du compte bancaire, crédits et dettes, fréquence des impayés et allocations sociales).

D'un autre côté, il y a les données subjectives comme les préférences et centres d'intérêts (orientation sexuelle, préférences alimentaires, vestimentaires et culturelles), les opinions et activités politiques ou religieuses (croyances intimes déclarés ou manifestés publiquement, signature d'une pétition). Il y a aussi des données comportementales tels que l'apparence, l'élocution et style de langage, types d'achats et établissement fréquentés, la consommation d'électricité et d'eau ou même la consommation de drogues. Et les données géographiques (lieux de retrait d'argent, lieux de paiement par carte comme les péages) et les données relationnelles comme la taille du réseau social, fréquence des rencontres, le nombre d'amis ou de partenaires sexuels etc....

On en déduit à travers cette classification des données personnelles qu'elles sont classées en deux catégories distinctes ; tout d'abord les données personnelles identifiantes qui sont les données rattachées directement à l'identité d'une personne toutes les données ou fichiers permettant d'identifier indirectement une personne, via par exemple un numéro d'identification, une adresse IP etc. Et puis les données comportementales qui sont rattachées à l'ensemble des comportements d'un individu, collectées via le suivi de ses navigations, mettant en avant ses comportements d'achats.

## **2. Les Différents Statuts d'une Donnée Personnelle**

La donnée personnelle est nécessairement liée au référentiel culturel des individus et à la réglementation en vigueur dans chaque pays. En économie, c'est un aspect essentiel à prendre en compte quand une société s'adresse à un marché international. Nous pouvons questionner trois perceptions relatives de la donnée personnelle qui impliquent trois approches différentes de la problématique :

- A l'échelle de l'entreprise : la donnée personnelle a une valeur stratégique et marchande. Elle permet de développer ou d'améliorer les modèles serviciels, d'enrichir l'expérience client, d'être analysée à des fins décisionnelles, d'opérationnalisation, de revente etc. Chaque

entreprise fait donc un travail de définition en contexte, en rapport avec le business qu'elle souhaite développer.

- A l'échelle du client : ses données personnelles sont une émanation de sa personnalité et de sa vie privée, une « trace » de ses comportements. C'est évidemment un point sensible. La confiance qu'il accorde dans les services numériques est fragile si la transparence, les finalités de traitement et les conditions de consentement ne sont pas claires (nous avons apporté une explication détaillée dans la sous partie III concernant le dilemme du consommateur).
- A l'échelle juridique : le statut juridique de la donnée personnelle permet de faire face aux problèmes qui existent entre la protection de la vie privée et l'autonomie des personnes et les besoins du marché d'utiliser leurs données pour développer de nouveaux services et créer de la valeur dans le marché.

La donnée personnelle offre une vision fermée de la donnée. Or, aujourd'hui, ces données sont ouvertes, elles circulent et se partagent en permanence. La notion même de donnée personnelle ne correspond plus à la réalité. Parler de données personnelles n'a plus de sens, il faudrait plutôt parler de données relationnelles, transactionnelles puisque les données circulent en permanence et qu'il est possible de déduire des informations personnelles à partir de données non personnelles. Le véritable enjeu se trouve dans l'interopérabilité des données.

## **II. Les Stratégies de Collecte des Données Personnelles**

### **1. Connaissance des Règles à Respecter**

La collecte des données s'effectue généralement directement auprès des personnes concernées et s'accompagne de mesures d'information. Elle peut aussi s'avérer indirecte c'est-à-dire réalisée à l'insu des intéressés. Il en est ainsi lors de traitements effectués à partir de cessions de données, hypothèse caractéristique des traitements de marketing mais qui ne se rencontre pas, à notre connaissance, dans le secteur de l'enseignement et de la recherche. En revanche, deux méthodes de collecte indirecte soulèvent des difficultés particulières dans ce secteur : l'extraction de fichiers par extension de finalité et le traçage électronique. Pour

collecter les données personnelles, la loi a fixé des règles sur le traitement, la collecte et la conservation de ces données que les entreprises concernées doivent respecter telles que veiller à la sécurité des fichiers, assurer la sécurité des données collectées, demander l'autorisation à la Commission nationale de l'informatique et des libertés (Cnil), fixer une date de conservation raisonnable des données périssables, définir un objectif précis au traitement et à l'utilisation des données, la proportionnalité et la pertinence des données collectées, La durée de conservation des données, La sécurité et la confidentialité des données, le respect des droits des personnes. Ainsi, une entreprise devra respecter ces principes et, la plupart du temps, informer la Commission de Nationale de l'Informatique et des Libertés (CNIL) de la collecte et du traitement de ce type de données. Il est très important de se mettre en conformité avec les règles dictées par la CNIL.

## **2. Sources et Outils de Collecte des Données Personnelles**

Les données personnelles collectées sont avant tout caractérisées par une grande diversité de la nature des données et surtout de leurs sources : « données transactionnelles, données collaboratives, données issues des systèmes de gestion, registres officiels, médias sociaux, données issues de capteurs et objets connectés, traces numériques, etc. Les données personnelles proviennent d'une part des individus qui dévoilent d'eux-mêmes sur internet : données déclaratives, questionnaires, inscriptions en ligne (de façon volontaire ou involontaire) ... Mais les données personnelles s'étendent bien au-delà de cette sphère déclarative. Les êtres humains ne sont plus les seuls producteurs de données, car les machines en produisent également à travers différents types de capteurs ou d'objets connectés et qui révèlent parfois plus d'informations personnelles grâce aux techniques de Data Mining, capables de corrélérer des données de manière informelle et d'en tirer de nouvelles informations. D'autre part, la façon dont les données sont produites n'est pas toujours, pour leurs auteurs, consciente ou volontaire, et pourtant toutes les traces numériques issues de leurs requêtes sur les moteurs de recherches, tous leurs « clics », parcours de navigation ou l'activation de la géolocalisation génèrent autant de données, qui peuvent être ou non associées à une identité physique, via l'adresse IP notamment. Les entreprises utilisent aussi la gratuité de leurs services pour attirer les internautes en les poussant à dévoiler des informations les concernant (e-mail, réponses à quelques questions, sondages etc...) afin de profiter d'un service gratuitement.

Si l'entreprise ne dispose d'aucun fichier, elle peut en louer ou en acheter auprès de fournisseurs. Sinon, elle peut récolter elle-même des données auprès de ses clients qui sont là pour un service quelconque. Elle dispose alors de plusieurs façons de récolter des données tel que la mise en place de campagnes de marketing direct (séminaire, jeux, concours, etc.), un programme d'affiliation, des partenariats/du sponsoring, les réseaux sociaux (à travers, par exemple, une page Facebook ou Instagram dédiée à l'enseigne).

Chaque entreprise doit veiller à bien cibler ses clients (ou clients potentiels), puis à bien choisir les outils de collecte, la collecte massive de ces données doit avant tout bénéficier aux consommateurs tout en créant de la valeur à l'entreprise grâce au ciblage effectué, cela va diminuer les coûts de marketing et donc augmenter le profit de l'entreprise. Il est important que les entreprises communiquent à ce sujet. La collecte des données doit être loyale et transparente, il faut que l'entreprise informe les consommateurs sur la collecte (charte de confidentialité par exemple).

### **3. Traitement et Tri des Données Personnelles**

Une fois les données collectées, les entreprises doivent trier et traiter ces données car certaines d'entre elles peuvent présenter un risque pour l'entreprise comme une atteinte aux droits de la propriété intellectuelle, Il peut s'agir de la reproduction de textes protégés par le droit d'auteur, ou encore du logo d'une entreprise sans autorisation et de manière illicite ou tout simplement une usurpation d'identité et cela peut se traduire, par exemple, par la création de fausses pages ou de faux comptes sur un réseau social. Les données personnelles sont évolutives, Il ne sert donc à rien de les conserver sans effectuer une mise à jour régulière.

Chaque base de données a besoin d'être sans cesse enrichie, via un ou plusieurs canaux de communication. Par exemple, si certaines informations manquent aux données personnelles de ses clients, l'entreprise peut mettre en place la technique de l'appending qui consiste à récupérer des adresses e-mails pour les ajouter à sa data... De plus, les détenteurs de fichiers à caractère personnel doivent fixer une durée de conservation raisonnable comme préciser auparavant. Enfin, il ne faut surtout pas conserver des données plus longtemps que la durée

déclarée car cela est puni par le Code pénal de cinq ans d'emprisonnement et de 300 000 euros d'amende.

### **III. Les Modes De Production et Entreprises Concernées**

Une fois toutes ces données collectées par les entreprises on se pose des questions sur l'usage et l'exploitation qu'elles vont faire de ces données .Effectivement cela intéresse beaucoup les économistes , tout d'abord sur un plan économique et ceci représente tout un pan de la réflexion en économie sur les modèles économiques et les modèles d'affaires numériques , mais aussi un plan sociologique dans le sens où l'on a cette profusion de données par les individus c'est à dire que les agents économiques (y compris les entreprises) ont intérêt à ce que ces données soit produites , on se pose également des questions sur les comportements qui concourent à la production de ces données personnelles et en particuliers quelles sont les raisons pour lesquelles les individus ont autant besoin de se surexposer , et pour quelle raison y a-t-il un dévoilement de soi aussi important sur le web ?

Historiquement ce sont les administrations qui s'intéressaient aux données personnelles mais de nos jours les entreprises aussi tendent des perches aux individus qui ont tendance à se surexposer et donc involontairement à se sous-protéger et à savoir que la valeur des réseaux sociaux numériques est quasiment nulle si les utilisateurs ne dévoilent rien d'eux-mêmes mais ils le font en raison de la gratuité des services proposés par ces réseaux.

#### **1. Production Massive des Données Personnelles**

Nous allons mettre de côté les organismes administratifs et étatiques qui ne font pas cela pour des raisons économiques mais surtout pour la sécurité publique et la surveillance. Donc ce qui nous intéresse est le point de vue économique c'est à dire du côté des entreprises ; il faut savoir que ces données ont un potentiel gigantesque qu'elles soient anonymes ou personnelles elles représentent des enjeux économiques et sociaux très importants puisqu'elles sont à la source de nombreux nouveaux services. Ce développement pourrait être positif pour les uns et négatif pour d'autres comme par exemple sur le marché du travail si l'employeur cherche à récolter un maximum de données sur ses futurs employés (via les

réseaux sociaux), cela est positif pour l'entreprise mais négatif dans le cas où vous cherchez du travail, et cela permettra de générer plus de valeur.

En terme de sécurité, les données personnelles pourraient aider les états à mieux sécuriser le pays, il y a aussi l'exemple des cartes du crime en big data accessible à toute la population qui pourrait notamment servir pour les investisseurs immobiliers afin de mesurer l'hostilité de la ville (viols, crimes, etc..) dans laquelle ils investissent par contre cela remet en question la vie privée de certains individus, on en parlera prochainement dans la partie concernant les externalités des données personnelles. L'économie de la donnée nous fournit des exemples de monétisation de la donnée soit par des achats de base de données, soit par l'achat d'applications avec des bases clientes importantes. Nous en avons aussi le prix dans le darknet : on peut ainsi connaître la valeur marchande d'une adresse e-mail, d'un numéro de compte bancaire, etc.

Nous aurions tort de ne pas considérer la donnée comme un bien assez précieux qui relève du domaine de la propriété et qui se vend. Mais il est à noter que cette collecte massive pourrait être la source d'une pollution numérique et de risques sociétaux importants, au niveau journalistique on met en avant la surveillance planétaire en pointant les risques probablement en causant un dommage réel à la société.

## **2. Entreprises Concernées et Modèles d'Affaires**

L'exploitation des données personnelles a permis à certains modèles de business de se réinventer, voire de se créer, impulsant ainsi une nouvelle dynamique dans l'économie numérique. En témoigne en particulier l'explosion de deux modèles économiques :

- Les modèles bifaces : Google et Facebook sont typiquement des entreprises bifaces, c'est-à-dire qu'elles font de l'intermédiation entre deux types d'acteurs, les utilisateurs et les annonceurs. Ce modèle économique n'est pas propre au numérique, il existait déjà dans l'économie des médias et dans la banque de détail. 95,8 % des spécialistes du marketing considèrent Facebook comme le réseau social le plus efficace ce qui n'est pas étonnant, puisque le réseau de Mark Zuckerberg est aussi le plus populaire sur la planète, avec 2,2 milliards d'utilisateurs actifs mensuels. Cela, en grande partie grâce aux Facebook ADS : la régie

publicitaire de la plateforme brille par son efficacité, notamment en raison du nombre d'utilisateurs et de la précision de ses options de ciblage qui sont basées sur les différentes données personnelles que Facebook détient sur ces utilisateurs. La grande force des Facebook ADS réside donc dans la qualité du ciblage des annonces, ce sont les fameuses audiences personnalisées. Plus d'une trentaine d'attributs peuvent être croisés pour cibler les audiences sur le réseau (attributs démographiques, intérêts, comportements de soi et de l'entourage, etc.).

- Les modèles serviciels : les données participent grandement au mouvement de « servicialisation », c'est-à-dire le fait de « vendre un produit sous la forme d'un service. L'exemple des assurances est instructif : plutôt que de spéculer sur l'accidentologie pour établir leurs tarifs, les sociétés se basent désormais sur l'analyse des usages réels des dispositifs, grâce aux capteurs et objets connectés qui transmettent les données de conduite, de kilométrage etc.

## AXE 2 : Stratégies d'exploitation, Externalités et Dilemmes du Consommateur

Suite à la collecte des données, nous allons savoir dans ce chapitre les stratégies déployées dans l'exploitation des données personnelles par les firmes, les différentes externalités positives et négatives d'un point de vue exploitant et consommateur et finalement, le dilemme auquel les individus font face.

### **I. Les Stratégies des Entreprises : Discrimination des prix et Personnalisation/Publicité Ciblée et Marketing**

Dans ce chapitre, nous allons poursuivre notre étude sur le comportement des entreprises dans le marché des données personnelles, tout en parlant de leurs différentes stratégies suite à l'exploitation de ces données.

La personnalisation des offres et des produits à des fins marketing est un pilier de l'économie des données personnelles. L'analyse comportementale peut permettre de développer des modèles prédictifs pour être proactif dans la relation client et pouvoir augmenter ainsi ses propres bénéfices.

#### **1. La discrimination par les prix**

Il existe trois types de discrimination, et celui qui nous intéresse le plus dans notre étude et la discrimination du troisième degré. C'est-à-dire que les prix sont fixés en fonction d'un critère du consommateur comme l'âge, la situation géographique, le sexe...

L'objectif des firmes est de collecter les informations significatives sur les consommateurs afin d'évaluer leur aptitude à payer un bien et tarifier au niveau de cette disposition à payer et ainsi capter le surplus du consommateur.

Odlyzko (2003) considère que cette stratégie entraînerait une augmentation du bien-être social. En effet, une tarification unique exclurait un certain nombre de consommateurs dont

le prix du bien convoité serait au-delà de leur disposition à payer. Toutefois un certain nombre de conditions doivent être réunies pour que cette stratégie n'affecte pas le bien-être social.

Par exemple, si on prend le cas de deux consommateurs, auquel on tarife à  $T_1$  et  $T_2$  avec  $T_1 > T_2$  et que le coût marginal de la firme est noté  $C_m$ , il faudrait soit que  $T_1 > T_2 > C_m$  soit que  $T_1 - C_m > T_2 - C_m > 0$ .

Enfin, nous pouvons évoquer la discrimination intertemporelle que pratiquait Amazon en 2000. Il s'agissait d'établir une discrimination par les prix sur « deux périodes » afin de déceler la disposition à payer des consommateurs. Les consommateurs fidèles se voyaient proposer des prix plus élevés que les nouveaux consommateurs.

## 2. La Personnalisation des Services

La personnalisation consiste à proposer un service en prenant en considération les besoins ou les préférences des consommateurs. Sackman et *al.* (2006) cités par Rochelandet (2010) définissent trois stratégies de personnalisation :

De prime abord, les services personnalisés qui se basent sur l'exploitation directe des données personnelles.

Ensuite, les services individualisés qui se basent sur l'exploitation de données contextuelles non-relées à l'identité d'un individu. Par exemple, lorsqu'un consommateur se rend sur un site d'informations et consulte une page concernant le transport ferroviaire, il pourra voir s'afficher une publicité pour la vente de billets de trains.

Finalement, les services universels « *accessibles à chacun et reposant sur des données individuelles émises et utilisés par les individus eux-mêmes (commentaires postés sur des forums* » (Rochelandet, 2010, p.63).

## 3. La publicité ciblée

De nos jours, l'efficacité devint un mode de travail incontournable et préféré des entreprises. En effet, les sociétés les plus importantes d'Internet, comme Google ou Facebook, souhaitent rendre la publicité la plus efficace possible. La publicité ciblée vis-à-vis de l'Internaute s'avère donc être un moyen inéluctable pour des raisons économiques. Parmi celles-ci : l'intérêt de

l'annonceur est d'augmenter le taux de clic (ou d'achats), et donc également de cibler la publicité en fonction de l'utilisateur.

La CNIL (2009) a défini les quatre stratégies des entreprises en matière de publicité.

Premièrement, la publicité comportementale. Amazon est adepte de cette stratégie car elle fait des suggestions d'achat en fonction de ses achats précédents.

Deuxièmement, la publicité comportementale en réseau avec un degré de complexité supérieure. Une entreprise place des cookies traceurs à différents internautes formant ainsi un réseau de consommateur. Ensuite, la firme analyse l'évolution de leur comportement et leur envoie des publicités en fonction de certains critères tels que l'âge, le sexe.

Troisièmement, la publicité contextuelle qui consiste à proposer des publicités en fonction des mots que l'on saisit ou du sens des phrases.

Finalement, La publicité personnalisée comme la pratique Facebook qui propose des publicités en fonction de différents critères tels que l'âge, le sexe, la localisation qui s'avèrent des données saisies lors de l'inscription dans le site.

Comme résultat de ces stratégies, les entreprises catégorisent deux types de consommateurs :

« - **Les profils prédictifs** : ces profils sont établis par inférence en observant le comportement des internautes dans le temps, notamment en suivant les pages visitées et les publicités qui ont attiré son attention.

- **Les profils explicites** : ces profils sont établis à partir des données personnelles que l'internaute a lui-même fournies à un service web, notamment à travers son inscription » (CNIL, 2009).

#### 4. Marketing – Algorithme Comportement Client

L'analyse comportementale peut porter sur des données non-structurées et permettre de développer des modèles prédictifs pour être proactif dans la relation et la connaissance client. De nombreux modèles existent, mais nous pouvons citer dans le cadre de cette étude les résultats rendus publics des chercheurs iraniens des universités Azad et Alzahra à Téhéran : ils ont pu créer un algorithme de modélisation des comportements clients par l'intégration de données non balisées à un classificateur de données balisées.

Ce modèle permet « d'affiner les tendances et les modèles de prédiction, en vue d'un usage marketing » selon plusieurs chercheurs. Ce modèle d'analyse des données et de comportements clients est publié dans les études 'Advances in Information Sciences and Service Sciences'. Ci-dessous le schéma descriptif de ce modèle.

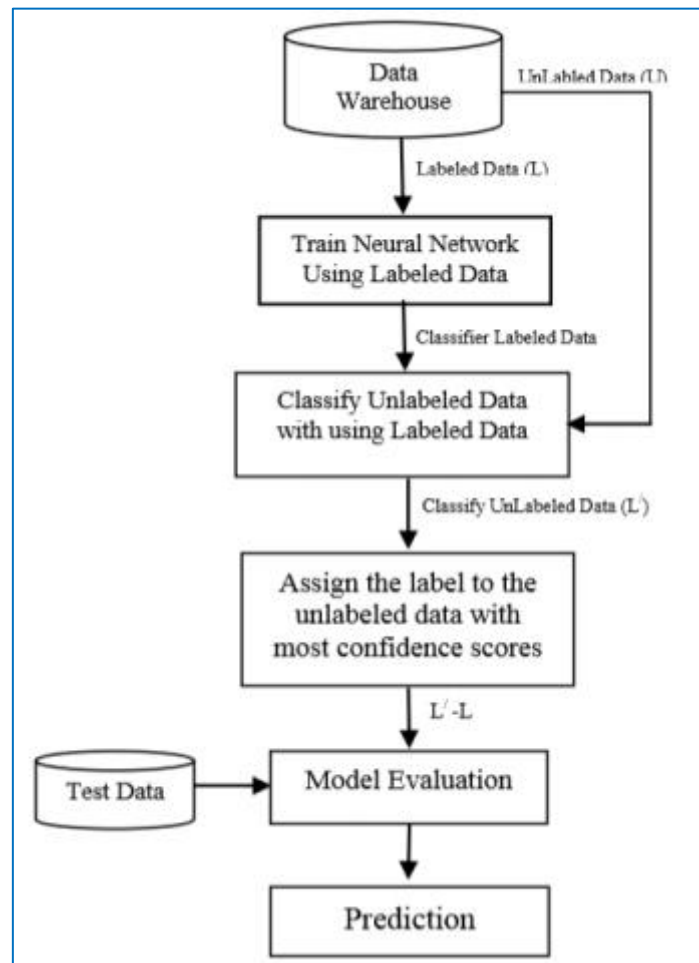


Figure1 : Algorithme de modélisation des comportement clients

Source: Customers Behavior Modeling by Semi-Supervised Learning in Customer Relationship Management<sup>(6)</sup>

Ce schéma nous montre que l'algorithme repose sur un réseau neuronal utilisant des données déjà annotées. Les données non balisées sont alors traitées et classifiées par rapport au classificateur initial de données balisées. Un nouveau classificateur est ainsi créé, regroupant les données balisées et celles nouvellement balisées. Ce système permet d'acquérir un meilleur degré de confiance et de précision pour l'évaluation des modèles, notamment des modèles prédictifs.

## II. Les Externalités des Données Personnelles :

Les externalités traduisent la variation de l'utilité d'un agent sans que cette variation passe par un prix, autrement dit par les mécanismes du marché. Cela permet de mieux appréhender le développement durable et de comprendre la nécessité d'inventer des modèles économiques plus vertueux pour les entreprises.

Concernant l'externalité de réseau, cela signifie que l'utilité d'un produit est liée positivement au nombre de consommateur possédant le même produit.

Par exemple : plus il y a de personnes sur Facebook, plus c'est intéressant de s'y inscrire soi-même (car la probabilité de retrouver ses proches augmente), donc plus de personnes vont s'y inscrire, renforçant encore l'intérêt du réseau.

***Olivier Simard-Casanova, un économiste et intellectuel libéral français*** : « Les externalités de réseau sont à l'origine d'effets boule de neige. »

Dans le cadre des données personnelles, on retrouve à la fois des externalités négatives et des externalités positives.

L'exploitation des données personnelles peut créer du bénéfice pour les firmes qui exploitent ces données.

En effet, les données personnelles peuvent être exploitées par les organisations comme un actif ou comme une source d'externalités positives. Leur utilisation en tant qu'actif entraîne des changements positifs au sein de l'organisation tandis que leur utilisation comme source d'externalités positives a un impact plus large sur l'économie et la société dans son ensemble.

### 1. Données personnelles = Actif ? :

Pour générer ces externalités, il convient de fluidifier la circulation des données personnelles, en les partageant ou en les rendant ouvertes. Les données personnelles deviennent alors un actif :

- Lorsqu'elles sont utilisées pour améliorer l'allocation des ressources ou les processus et pour réduire les coûts de transaction dans un objectif de gains d'efficacité ;

- Lorsqu'elles sont utilisées pour améliorer et personnaliser les services afin d'en accroître la qualité ;
- Lorsqu'elles sont utilisées comme élément de l'analyse prédictive visant à étayer la prise de décision et à améliorer la pertinence de cette dernière ;
- Lorsqu'elles sont utilisées pour mener des recherches en sciences sociales et établir des modèles comportementaux.

L'exploitation des données personnelles peut donc être considéré comme étant une externalité positive si l'organisation en question en tire un bénéfice net, notamment grâce aux coûts de cette opération qui s'avèrent négligeables (maintenance d'une base de données par exemple).

## **2. Prospection directe et Spamming**

De nos jours, l'attention devient une denrée rare et nous allons consacrer un chapitre sur cette ressource dans notre étude. Elle s'avère être l'objectif principal des deux types de prospection : le marketing direct et le spamming.

Les deux approches permettent de véhiculer des messages publicitaires non sollicités pour faire la promotion commerciale des produits. Bien qu'elles soient basées sur un modèle économique similaire, le spamming génère des externalités négatives plus importantes que celles du marketing direct.

En effet, grâce aux données personnelles, la prospection directe peut générer des bénéfices importants. Cela peut arriver car l'envoi de mails en masse engendre un coût négligeable alors que la transformation du message en actes d'achats peut être bénéfique à la firme en question.

Par conséquent, plus la qualité des données personnelles est optimale plus ce taux de transformation est important, car les destinataires et les préférences seront mieux ciblés.

Quant au spamming, la probabilité de réaliser des ventes est plus faible car il y'a plus de challenge pour cibler les destinataires qui seront amenés à consommer et moins de chances qu'ils réagissent positivement à cette publicité non désirée.

Toujours est-il, les entreprises qui ont recours à ces démarches risquent d'avoir leur réputation entachée auprès des consommateurs, ce qui peut s'avérer une externalité négative.

### **3. Abondance des informations/Economie de l'Attention**

La prospection directe, abordée dans le paragraphe précédent, engendre des externalités négatives de production entre les entreprises elles-mêmes.

En effet, la surinformation s'avère être une externalité négative pour les exploitants qui doivent cibler les messages en fonction des préférences des receveurs, ce qui impose une surexploitation des données personnelles.

Bien que les coûts de collecte des données personnelles soient identiques, quel que soit leur degré d'exploitation, les entreprises ont tendance à investir dans le marketing, ce qui engendre des coûts conséquents sans résultat garanti. En effet, les promotions excessives incitent les consommateurs à ignorer tout message.

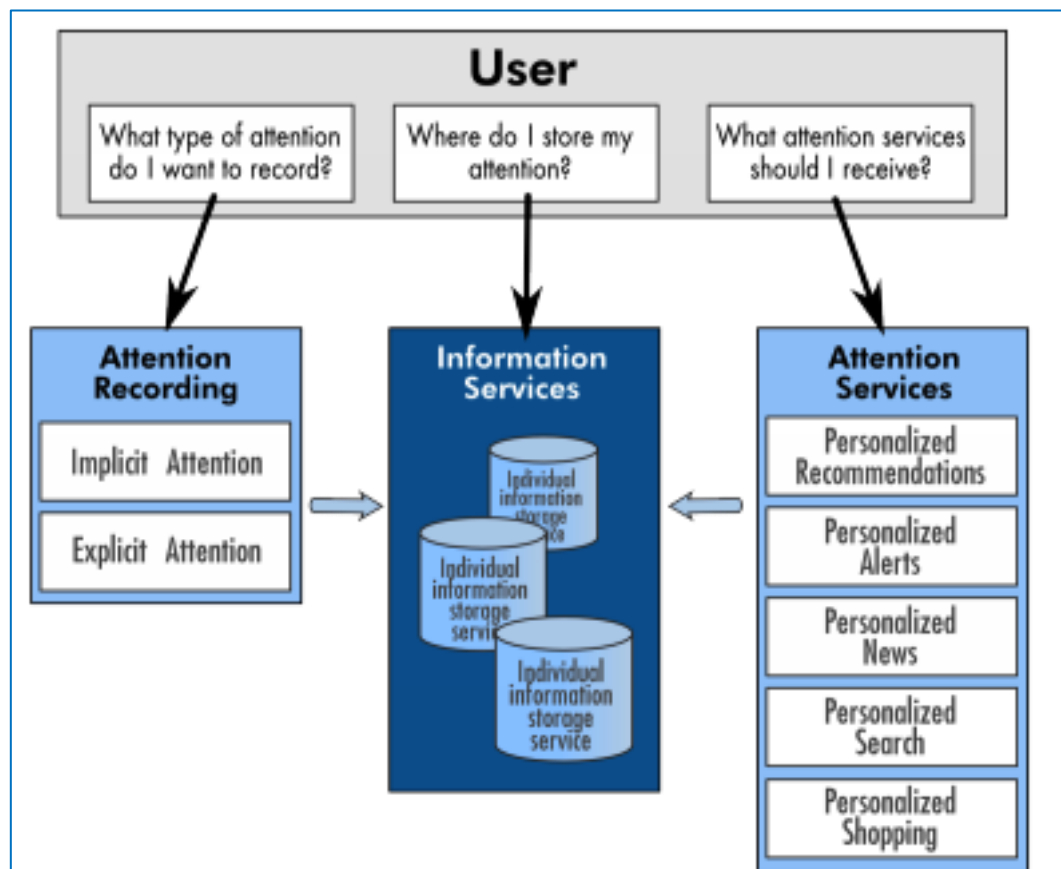


Figure2 : Modèle Américain de l'Economie d'Attention

Herbert Simon, économiste et sociologue américain, ayant forgé un concept de rationalité limitée, qui porte sur l'étude du comportement d'un individu face à un choix a dit :

« Dans un monde riche en informations, l'abondance d'informations entraîne la pénurie d'une autre ressource : la rareté devient ce que consomme l'information. Ce que l'information consomme est assez évident : c'est l'attention de ses receveurs. Donc une abondance d'informations crée une rareté de l'attention et le besoin de répartir efficacement cette attention parmi la surabondance des sources d'informations qui peuvent la consommer ».

### III. Le Dilemme du Consommateur

Des études ont montré que les internautes attachent une valeur très importante à leur vie privée, notamment la protection de leurs données personnelles sur Internet. C'est ce qui peut

leur amener aux méfiances des achats en ligne, par peur de nuisance ou des problèmes via leur cartes bancaires, donc méfiance de piratage par exemple, ou de réception de publication non désirés (par exemple les spam). Ils seront donc disposés à payer pour protéger leurs données personnelles

Par contre, quelques expérimentations ont montré que les internautes exigent un prix plus élevé afin de céder leurs informations personnelles si quelques entreprises comptent les exploiter par rapport à la somme dont un internaute est prêt à payer afin de protéger ses données personnelles contre toute forme de collecte et d'exploitation. Ou encore, lorsque l'internaute possède les droits de propriétés sur ces données personnelles, alors la disposition à accepter l'utilisation de ses informations est plus élevée à la disposition à payer pour la protection de ses données contre toute utilisation.

On se pose alors la question, pourquoi bien que l'individu sache les impacts de l'exploitation de ses données personnelles, il continue toujours à les céder sans méfiance ?

## **1. Comportement des Individus**

Des études ont montré l'existence d'une surexposition de soi sur internet. Les internautes laissent derrière eux plusieurs traces, et cela nous conduit à s'interroger sur les raisons, les motivations d'un tel comportement.

L'angle de la raison conduit à remettre en cause l'hypothèse fondamentale de la rationalité de la théorie standard en économie. Cette théorie normative permet de prédire les comportements, elle repose notamment sur l'hypothèse de l'homo economicus consistant à supposer que l'individu est :

- Rationnel (qui optimise ses choix et qu'il est cohérent)
- Calculateur (qui parvient à faire des arbitrages et qu'il réagit en fonction des incitations)
- Egoïste (qu'il agit dans son intérêt)

D'autres études ont montré qu'il existe une disparité entre la disposition à payer pour se protéger et la disposition à vendre une information alors que la théorie standard prévoit qu'il

y ait égalité. Les individus sont alors prêts à céder leurs informations contre une très faible contrepartie (comme pouvoir communiquer via un réseau social ou maintenir un blog), et sont généralement indifférents à la protection de ces informations.

Ces dernières études vont démontrer les écarts par rapport à la théorie standard, qui juge égales la disposition à payer et celle de protéger la vie privée. Ils vont proposer quelques hypothèses :

- L'illusion du contrôle et l'effet de valence

L'idée du choix de diffuser une information conduit l'individu à penser qu'il maîtrise les risques. L'effet de valence suppose que l'individu surestime les événements favorables.

- Sous-Evaluation des risques cumulatifs

La configuration d'un site influe sur le comportement des individus et les conduit à agir différemment selon que le site semble sérieux ou amusant.

- L'ignorance rationnelle

*« Ainsi, ne pas lire la politique de confidentialité d'un site Internet est rationnel, si l'individu estime que la longueur et donc le coût de lecture et de compréhension de ce texte surpassent les avantages inhérents à la consultation du site » (Rochelandet, 2010, p.84)*

Le comportement du consommateur soulève d'autres questions, parmi celles-ci on peut se demander si un profilage excessif des individus ne les conduiraient pas à adopter de manière systématique de nouveaux produits et conduiraient ainsi au conformisme.

## 2. Bien-être des Consommateurs

D'un point de vue consommateur, comme indiqué dans l'Axe 1, ses données personnelles sont une émanation de sa personnalité et de sa vie privée, une « trace » de ses comportements. C'est évidemment un point sensible qui risque d'impacter le bien être des consommateurs.

En effet, les destinataires d'emails, courriers ou d'appels téléphoniques doivent consacrer du temps et de l'attention afin de répondre, trier les messages ce qui crée du désagrément coté consommateur. Ce désagrément est d'autant plus accentué que les messages sont non-sollicités et des fois sans aucun rapport avec leurs besoins (spamming).

Leur bien être est alors affecté par l'intrusion dans leur vie privée.

Si le message véhiculé risque de susciter un intérêt chez le client, cette gêne peut alors être minimisée et le bien être peut être considéré alors augmenté.

De plus, les vendeurs disposant des données personnelles des individus vont contacter les consommateurs (via email ou téléphone), leur imposant des coûts et atteignant alors leur bien être psychologique et financier :

- Coûts non monétaires : Coût de l'attention, perte de temps liée au tri et à l'élimination, interruption dans son activité par un appel téléphonique, agacement...

- Coûts monétaires : filtres anti-spamming, recyclage de papiers, frais téléphoniques éventuels...

L'autonomie des individus peut donc être mise en cause à cause de certaines activités qui peuvent résulter de l'exploitation des données, comme les escroqueries en ligne, l'usurpation d'identité, chantage etc.

Par ailleurs, puisque les entreprises pratiquent la discrimination par les prix, grâce à la collecte des données personnelles, cela peut s'avérer bénéfique au bien-être des consommateurs à faible disposition à payer, qui ne seraient donc plus exclus du marché mais se verraient alors proposer des prix adaptés.

### AXE 3 : La Protection des Données et ses Effets Face Au Marché

Les entités impliquées dans le domaine internet telles que les sociétés dont l'activité commerciale se déroule partiellement ou totalement en ligne collectent une grande quantité de données notamment de particuliers-utilisateurs de ces plateformes, or la loi, entre autres fonctions, a vocation à protéger la vie privée des personnes. Et dans les plateformes numériques en particulier, le droit impose un cadre juridique particulier à suivre « à la lettre » sous peine d'être sanctionné.

Ces contraintes sont englobées dans la notion de « confidentialité ». L'Organisation Internationale de Normalisation la définit comme « le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé ». Dans le commerce en ligne, la confidentialité va de pair avec la notion de « sécurité » qui consiste à réduire les menaces sur la protection des données personnelles par des stratégies et des outils juridiques.

Le but de la loi est d'encadrer l'utilisation de ces données personnelles, et surtout de valoriser avant tout l'information et le consentement des personnes concernées. Par ailleurs, cela implique également la lutte contre la mauvaise utilisation des données et le piratage des données.

En France, c'est la CNIL, Commission Nationale de l'Informatique et des Libertés, une autorité administrative indépendante qui se charge d'empêcher l'informatique et la révolution numérique de porter atteinte à la vie privée des personnes et à leurs libertés individuelles. S'ajoutent aux dispositions nationales les dispositions de l'Union Européenne à ce sujet. La CNIL met à disposition des entités responsables du traitement de données un cadre de conduite et de conformité et fournit également de la documentation et du conseil.

#### **I. La Confidentialité/Traitement des Données Personnelles : Contraintes et Limites Juridiques pour les Entreprises**

D'un point de vue commercial, les entreprises portent un intérêt majeur aux données personnelles des utilisateurs de sites internet, (clients, prospects), car une fois collectées, elles permettent de les utilisées à fins de marketing stratégique : elles permettent en effet de cibler

des segments de clientèle et mener des études de marché efficaces. Les entreprises peuvent alors mieux connaître leurs consommateurs et adapter leurs produits. Cependant, une mauvaise exploitation de ces données peut exposer l'entreprise à des risques importants pouvant être à l'origine de destruction de valeur.

Les entreprises perçoivent la loi encadrant le traitement des données personnelles comme une contrainte au développement économique, la réglementation ne manque pas de prendre en compte les intérêts des entreprises et de s'adapter au progrès technologique. C'est pour cela que des solutions technologiques tentent d'apporter des réponses à ces problématiques, par exemple : le « fast data » est un processus qui permet le traitement court des données et celles-ci sont supprimées immédiatement après leur utilisation.

Les contraintes juridiques concernant la confidentialité peuvent s'articuler autour de trois axes : vis-à-vis de la loi, il existe des formalités obligatoires à respecter (mentions), en plus de l'obligation d'information des personnes concernées et des obligations spécifiques aux compagnes d'e-mailing.

## **1. Obligations vis-à-vis de la Loi**

C'est la loi Informatique et libertés du 6 janvier 1978 modifiée par la loi du 6 août 2004 qui installe le cadre juridique du traitement des données en ligne.

Selon cette loi, la constitution de fichiers clients à partir des données recueillies devra au préalable faire l'objet des formalités administratives introduites par le CNIL (Commission Nationale de l'Informatique et des Libertés, qui est un organisme qui accompagne les entreprises dans la maîtrise du traitement des données personnelles, afin de limiter l'impact des nouvelles technologies (innovations) sur les libertés et la vie privée.

Cette autorité nationale a établi dans son site un ensemble de normes, simplifiées, que les entreprises doivent respecter dans la gestion des clients et des prospects. Le responsable du traitement doit remplir formulaire d'engagement de conformité à la norme disponible sur le site de la CNIL : [www.cnil.fr](http://www.cnil.fr).

**Menu du formulaire**

- ✓ Changer de procédure
- ✗ **Déclarant**
- ✗ Finalité
- ✗ Contact
- ✗ Identification du responsable
- ✗ Validation et envoi

**Déclarant**

A savoir

Pour enregistrer le formulaire, saisissez les données obligatoires du déclarant.  
Les champs dont les libellés sont en caractères gras sont obligatoires.

**Champs obligatoires**

**Organisme Déclarant** ?

Cochez ci-contre ☐ si vous déclarez à titre individuel (vous n'avez pas de n° siren)

N° SIREN + NIC   ?

Code NAF/APE Choisissez

Nom/Raison sociale

Nom du service

Adresse

Code Postal

Ville

Sigle  ?

Téléphone

Télécopie   
(ne doit comporter que des chiffres)

Adresse électronique

Enregistrer

étape suivante >>>

Figure 3 : Formulaire d'engagement de conformité à remplir en ligne

La norme simplifiée N°48 établie les dates précises de conservation des données clients, selon que les données sont récoltées dans le cadre d'une transaction commerciale, d'un paiement bancaire ou d'une prospection, et selon que le responsable du traitement des données souhaite les utiliser à des fins de statistique, de prospection, de fidélisation, la durée moyenne étant de trois ans, après quoi les données doivent être anonymisées.

Les entreprises doivent avoir pris connaissance des paramètres de leur traitement de données et de la conformité de ce traitement aux normes établies avant d'engager les formalités auprès de la CNIL.

Compte tenu de ces paramètres, lorsque le traitement des données pourrait porter atteinte à la vie privée, la loi Informatique et libertés prévoit une obligation de déclaration et d'autorisation préalable.

La CNIL a mis à disposition des entreprises un guide, "Déclarer à la Cnil" afin d'orienter les entreprises dans l'accomplissement de ces démarches. Il faudra ensuite attendre l'accord de la CNIL (avec numéro d'identification), à défaut de quoi, le responsable s'exposerait à des sanctions pouvant aller jusqu'à cinq ans d'emprisonnement et 300.000 euros d'amende.

## 2. Obligations vis-à-vis des Clients/Prospects

En plus des formalités administratives, le responsable du traitement de données est par ailleurs tenu par une obligation de sécurité et de confidentialité des données : lesdites données doivent être préservées et ne pas parvenir à des tiers qui ne seraient pas autorisés à y accéder.

Par ailleurs, les personnes concernées doivent être informées de l'existence d'une collecte de données. Une liste d'informations à leur fournir est établie par l'article 32 de la loi Informatique et des Libertés.

**Chemin :**  
[Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés](#)  
▶ Chapitre V : Obligations incombant aux responsables de traitements et droits des personnes  
▶ [Section 1 : Obligations incombant aux responsables de traitements.](#)

**Article 32**  
Modifié par [LOI n°2018-493 du 20 juin 2018 - art. 23](#)  
Modifié par [LOI n°2018-493 du 20 juin 2018 - art. 29](#)  

I.-La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :

- 1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
- 2° De la finalité poursuivie par le traitement auquel les données sont destinées ;
- 3° Du caractère obligatoire ou facultatif des réponses ;
- 4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ;
- 5° Des destinataires ou catégories de destinataires des données ;
- 6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre dont celui de définir des directives relatives au sort de ses données à caractère personnel après sa mort ;
- 7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;
- 8° De la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée.

*Figure 4 : Extrait article 32 de la loi Informatique et Libertés*

Il faut également les informer de leur droit d'accéder aux données collectées et de les rectifier. De plus, avant la validation ou signature d'un contrat, les utilisateurs doivent avoir la possibilité de s'opposer à ce que leurs données soient utilisées à des fins de prospection commerciale.

Dans le cadre de collecte de données par des questionnaires ou formulaires en ligne, des « mentions CNIL » de prévention doivent apparaître de manière claire et lisible.



The image shows a web form for 'Association XYZ'. It includes input fields for 'NOM (OBLIGATOIRE)' and 'EMAIL (OBLIGATOIRE)'. Below these is a checkbox with the text: 'EN SOUMETTANT CE FORMULAIRE J'ACCEPTE QUE LES INFORMATIONS SAISIES SOIENT EXPLOITÉES POUR LES FINALITÉS DÉCRITES CI-DESSOUS.' A blue 'Envoyer' button is present. The form also contains a section titled 'Conditions d'utilisation de vos données personnelles' which states that the association will use the data to improve the user's experience and may communicate with them. It also mentions that the association is committed to protecting the confidentiality of the data and provides a link to their privacy policy.

Figure 5 : Exemple de « mention CNIL » établie par un responsable de traitement de données

Ainsi, dans le cadre du fonctionnement de leur activités, les entreprises sont tenues du respect de ces contraintes à chaque fois qu'elles envisagent d'exploiter des données personnelles, dans le cadre de statistiques ou de prospection.

### 3. Les Cookies

Les cookies sont des fichiers qui enregistrent les informations qu'un internaute introduit dans un site internet et celles liées à sa navigation sur ce site, ce qui lui permettra d'accéder plus rapidement à ce même site lors de sa prochaine connexion. Lorsque l'utilisateur accepte l'utilisation des cookies, l'entreprise aura le droit d'accéder à ces données et de les exploiter à des fins commerciales.

Cette fonctionnalité introduit de nouvelles contraintes juridiques liées à l'obligation d'information et la réquisition du consentement préalable avant l'exploitation des données personnelles.

Le droit applicable à l'utilisation des cookies sont les dispositions de l'article 32-II de la loi du 6 janvier 1978 ainsi que la recommandation n° 2013-378 du 5 décembre 2013 de la CNIL, comportant sept articles.

Les collecteurs de données sont donc tenus d'informer de « manière claire et complète » tout utilisateur du site que ses données et des informations liées à sa connexion sur le site, peuvent être stockées, s'il l'accepte. Celui-ci doit exprimer son accord préalable après avoir été informé, c'est ce qu'on appelle une « affirmation informée ».

L'expression de son consentement se fait par un système d'« opt-in ». En effet, l'information de l'utilisateur se fait en général par une fenêtre ou un bandeau s'affichant en bas de page (et comprenant un lien renvoyant aux conditions générales d'utilisation des cookies) lors d'une première connexion, visibles jusqu'à ce que l'utilisateur clique sur « J'accepte » ou le coche simplement.

Comme il n'existe pas de système « opt-out » (refus), la simple non-validation de l'acceptation vaut pour opposition de l'utilisateur à l'utilisation des cookies.

## **II. L'Innovation et La Conformité à la Loi**

Le progrès technologique et l'émergence par exemple des Big Data (large procédé de collecte d'importante quantité de données) soulèvent la problématique de l'adéquation de ces avancements à la loi informatique et Libertés, notamment concernant la finalité de cette collecte ; bien qu'au vu des moyens investis pour développer ce procédé et analyser le contenu, on peut déduire qu'il bien une finalité à cette collecte, ce principe est donc respecté.

Ainsi, Isabelle Falque-Pierrotin, Présidente de la CNIL, lors d'une conférence en 2014 disait à ce propos : *« L'idée que la CNIL s'opposerait aux aspects positifs en termes d'innovation qu'apporte le Big Data, n'est pas étayée par la réalité (...) Ces sujets (l'interconnexion de fichiers, la segmentation toujours plus fine des clients), ne sont pas en soi contraires à la Loi Informatique et Libertés. La seule chose que demande celle-ci, ce sont des garanties en termes de liberté des individus ».*

### **1. Sécurité des Données et Développement Technologique**

La régulation est indispensable pour protéger les libertés et la vie privée des utilisateurs de plateformes internet, cependant il est important que celle-ci puisse accompagner le

développement technologique et non le freiner ou obstruer les progrès de l'innovation (la CNIL a par exemple mis à disposition des entreprises la « boîte à outils conformité »). Le but de la CNIL est donc de s'adapter au développement, non pas en modifiant ses principes et objectifs de départ mais en développant de nouveaux outils de protection qui apportent des solutions aux problématiques modernes et accompagnent l'innovation dans le cadre d'un développement durable et éthique.

L'idée d'accompagnement est fondamentale, elle se traduit par une implication plus active de la CNIL. C'est dans cette logique que fut créé en 2012 le « pôle innovation et prospective » dont la fonction est d'apporter des conseils aux start up dès la phase de conception de leur produit afin d'assurer une fonctionnalité de protection optimale des données.

Ainsi, le but de la loi est d'assurer les objectifs de sécurité tout en prenant en considérant les enjeux du développement moderne.

Pour leur part, les entreprises françaises et européennes en générale, étant plus encadrées sur le plan juridique doivent trouver le moyen de transformer ces contraintes juridiques, « obstacle » à la compétitivité en avantage concurrentiel dans le contexte international.

En effet, outre la difficulté sur le plan stratégique marketing (prospection) et la complexité de poursuivre leurs projets numériques qui résultent de la réglementation, ce qui inquiète les acteurs économiques ceux sont aussi leurs concurrents internationaux notamment nord-américains qui sont soumis à une réglementation plus souple et flexible et sont donc plus compétitives et réactives car elles ont moins de restrictions et donc plus de libertés d'action. Cela soulève de nouveau la problématique de ces dernières années en France, celle de « l'équilibre à trouver entre modèles innovants (dynamiques mais parfois intrusifs) et protection de la vie privée (essentielle mais parfois pesante) ».

Cependant, comme l'explique Thomas Beaugrand, Avocat chez Staub & Associés, l'encadrement juridique n'a pas empêché les acteurs européens à s'intégrer dans le marché de l'innovation, bien au contraire ils y occupent une place importante. Et selon lui, ils devraient profiter de leur notoriété afin de faire valoir ces contraintes pour la protection des données

personnelles et les « *convertir (...) en avantages marketing et compétitifs, sous forme de « label qualité » par exemple* ».

Plusieurs initiatives sont développées dans ce sens :

- *Cloud Confidence* : label de confiance sur la transparence sur les règles de sécurité et de confidentialité des données
- *Label « Gouvernance Informatique & Libertés »* : proposé par la CNIL
- *Privacy by design* : principe de respect de la vie privée dès la conception du produit

Finalement, un équilibre entre révolution numérique et réglementation est encore possible, le défi étant d'assurer la durabilité de celui-ci en convergeant les intérêts de toutes les entités impliquées.

## **2. Innovation, Santé et Réglementation**

Les données personnelles liées à la santé des personnes sont considérées par le droit européen comme sensible et font donc l'objet d'une vigilance spéciale. Elles sont gérées par un prestataire agréé par l'Agence des systèmes d'information partagés de santé. Le traitement de ces données est interdit par la loi sauf si elles sont anonymisées ou dans certains cas spécifique (si le traitement a pour finalité un intérêt général, avec le consentement explicite des personnes concernées, ou s'il a un objectif de recherche ayant une mission de service public, par exemple).

Aujourd'hui le projet numérique touche également le domaine de la santé. De nombreux d'objets connectés permettent de quantifier des données personnelles liées à l'activité corporelle (« quantified self »), elles forment un nouveau type de données, les « données du bien-être et de mode de vie ». Des exemples d'objets qui impliquent ces données sont les bracelets connectés, podomètres, tensiomètres, moniteurs de fréquences cardiaques, ...etc. A ce jour, ces données de bien être ne sont pas considérées comme des données médicales et ne sont donc pas soumises à la même réglementation que ces dernières.

Néanmoins, il existe des « normes harmonisées » concernant le traitement de ces données qui ont été établies par la Commission Européenne afin d'aiguiller les développeurs de telles applications et objets et leur permettre de vérifier si les données qu'il récoltent relèvent de la réglementation sur les dispositifs médicaux ou dispositifs médicaux de diagnostic in vitro ou pas. Pour pouvoir relever de ces normes, il faut que les données collectées se limitent à des données physiologiques brutes n'aboutissant pas à des informations ou diagnostics médicaux.

Par ailleurs, la santé est devenue un enjeu important de l'économie numérique. La Commission Européenne ne nie pas la valeur économique apportée par les données de santé mobiles, notamment car elles favorisent la prévention, ce qui permet selon le livre vert de la santé publique de « mieux planifier les interventions, d'éviter les consultations inutiles et de mieux préparer les professionnels ». Sur le plan financier, cela permet de réduire les coûts liés à la santé des Etats et de l'UE en général.

Il est toutefois indispensable que les progrès dans ce domaine prennent en considération la confiance qu'auront les utilisateurs vis-à-vis du traitement de leurs données par les entreprises et les autorités publiques. Il est donc nécessaire de mettre en œuvre des moyens d'action réglementaire visant à assurer non seulement la sécurité de ces dispositifs mais également la transparence.

### **III. La Protection des Données dans le cadre de l'Union Européenne**

A l'image du droit national, le droit européen met également en place des textes qui réglementent le traitement des données personnelles.

En 1995, le Parlement européen a mis en place une directive, la Directive 95/46/CE, qui protège les personnes physiques vis-à-vis du traitement et de la libre circulation de leurs données personnelles. Celle-ci a récemment fait l'objet d'une révision, concluant par le Règlement (Européen) Général de Protection des Données (RGPD), appliqué depuis mai 2018 dans les Etats membres de l'Union Européenne. Selon la Commission Européenne, ce règlement a pour finalité de s' *« adapter aux nouvelles exigences liées au développement rapide des nouvelles technologies et à la mondialisation tout en veillant à ce que les individus*

*gardent un contrôle effectif sur leurs propres données : la proposition de la Commission concernant un règlement général sur la protection des données permettra d'harmoniser davantage les règles en la matière existant dans l'UE et, par l'établissement d'un niveau élevé et uniforme de protection des individus, garantira la sécurité juridique aux entreprises et suscitera une confiance accrue dans les services [...] en ligne. »*

Ce projet s'élabore autour de deux principaux axes. Le premier étant d'étendre l'intégration des pays membres de l'UE à l'avancement numérique et de créer une action commune et unifié pour la protection des données personnelles (concept de l'« l'Europe des données »). Le second axe est la concurrence des acteurs européens et internationaux, il s'agit d'appliquer le règlement (issu du droit européen) autant aux entités européennes qu'aux entités internationales adressant un produit ou service à un citoyen européen (y compris si leur siège est à l'étranger), afin que tous ces acteurs soient au même niveau.

Le projet européen suppose par la suite un investissement des régulateurs nationaux afin d'assurer la bonne application des dispositions qu'il comporte. En France, c'est la CNIL qui est chargée de contrôler le respect du règlement européen.



Figure 6 : Les principaux objectifs du RGPD

Les bases de ce projet s'articulent autour de 4 principes fondamentaux :

**-le principe d'Accountability** : selon lequel les sociétés qui traitent les données doivent répondre de leurs actions. Elles doivent se conformer à la réglementation sur la protection des données personnelles et montrer la conformité de leurs procédés en maintenant une transparence vis-à-vis des autorités régulatrices (assurer la traçabilité des données).

**-le Privacy Impact Assesement** ou l'Etude d'Impact sur la Vie Privée : il s'agit d'analyser les risques que peut avoir un produit/service (au cours de son développement) d'atteinte à la protection de la vie privée ; le but étant de prévenir ces conséquences en développement simultanément le moyen d'éviter la survenance de ces risques.

**-le Privacy by Design** : il s'agit d'assurer la conformité du produit au cadre juridique dès la phase de conception et tout au long du développement du produit ou service (exemple : prévoir les moyens de consentement des personnes concernées)

**-Le Data Protection Officer (DPO)** : il est désigné par l'entité qui traite des données personnelles, sa fonction est d'accompagner les entreprises dans leurs démarches de conformité à la loi. Récemment, sa fonction s'est néanmoins étendue à celle de contrôle et d'audit de l'entité.

Par ailleurs, le RGPD prévoit un ensemble de droits pour « la personne concernée » qui sont énoncés dans les articles 12 à 22 du règlement, parmi lesquels :

**-le droit d'accès aux données personnelles** : la personne dont on collecte les données peut obtenir confirmation que ses données sont traitées, peut accéder auxdites données et savoir la finalité de ce traitement pour la société (article 15)

**-le droit de rectification et droit à l'effacement (droit à l'oubli)** : la personne concernée a le droit de modifier et rectifier ses données afin de les actualiser, et par ailleurs demander leur effacement sous certaines conditions (par exemple lorsque la personne retire son consentement au traitement de ses données, ou s'oppose à ce traitement et à sa finalité, ou encore lorsque les données sont traitées dans un cadre illicite). Cependant, le droit à l'oubli est limité par l'article 17, il ne s'applique pas lorsque le traitement se fait dans le cadre du

droit à la liberté d'expression et d'information ou d'exercice ou de la défense des droits en justice.

**-le droit à la portabilité des données :** la personne concernée peut récupérer dans un format automatisé et lisible ses données personnelles fournies à un responsable de traitement et les utiliser à des fins personnelles ou les communiquer à un autre responsable de traitement sans possibilité pour le premier de s'y opposer.

**- le droit d'opposition :** la personne concernée a le droit de s'opposer à que ses données soient traitées y compris à des fins de profilage, comme le font certaines entreprises afin d'évaluer les performances de leurs salariés.

Si la personne concernée se voit violer son droit, des moyens d'action légaux sont à sa disposition. En effet, elle peut tout d'abord s'adresser à l'autorité nationale, la CNIL en France. Le régulateur a mis en place un système de dépôt de plaintes en ligne. En outre, conformément à l'article 79 du RGPD, la personne concernée peut intenter une action en justice. De plus l'article suivant ouvre la possibilité à des actions de groupe, en effet la personne concernée peut mandater un organisme à but non lucratif qui milite pour la protection des libertés et des données personnelles.

Ces actions peuvent engager des sanctions considérables pour les organismes collecteurs impliqués. Les sanctions financières peuvent aller jusqu'à 10 millions d'euros ou, pour une entreprise, 2% du chiffre d'affaires annuel mondial pour des manquements notamment au Privacy By Design ou Privacy Impact Assessment ; et jusqu'à 20 millions d'euros ou, 4% du chiffres d'affaires annuel mondial (pour les entreprises) pour manquement notamment aux droits des personnes (droits d'accès, de rectification, d'opposition, de suppression, droit à l'oubli, etc.). A cela s'ajoutent les conséquences sur la réputation de l'entreprise et son image de marque. En outre, il existe la possibilité pour les Etats membres de l'UE de déterminer les sanctions pénales à infliger à une entreprise qui aurait violé les dispositions du RGPD.

## CONCLUSION

Ce document a pour ambition de rappeler le contexte dans lequel peut se développer l'économie des données personnelles tout en abordant l'un des enjeux clés de l'économie numérique qu'est l'équilibre entre l'utilisation des données personnelles et la préservation de la vie privée.

Dans un monde de données personnelles partagées, un marché est en train de se construire exclusivement autour de la valorisation de ces données personnelles, les grandes entreprises ont aussi leur rôle à jouer dans cette économie via la redéfinition de leurs modèles d'affaire.

Ces firmes développent alors de multiples stratégies afin de mieux exploiter ces données pour que ce soit un facteur inéluctable de leur croissance. Cela crée des comportements ambivalents de la part des individus qui s'avèrent enclins à divulguer des aspects parfois intimes de leur vie privée et réticents à se protéger.

Enfin, un autre thème fondamental est celui du business éthique : le sujet de l'économie des données personnelles ne doit pas opposer business et éthique, ces deux dimensions doivent être pensées conjointement. Les entreprises doivent alors penser à une économie symétrique ; gagnant-gagnant, où les consommateurs/clients deviennent les premiers partenaires des entreprises et donc co-créeurs de valeurs.

## BIBLIOGRAPHIE ET WEBOGRAPHIE

- Livre rédigé par Fabrice Rochelandet, en Février 2010, intitulé "Economie des données personnelles et de la vie privée" de collection "Repères".  
ISBN : 978-2-7071-5765-2.
- Site de CAIRN.INFO : <https://www.cairn.info/Economie-des-donnees-personnelles-et-de-la-vie-pri--9782707157652-page-38.htm?contenu=resume#>  
Ce site explique l'exploitation des données personnelles, vie privée ainsi que ces externalités positives et négatives.
- [www.Cigref.com](http://www.Cigref.com) site concernant les réseaux des grandes entreprises.  
Tel : 0156597000  
Email : [contact@cigref.fr](mailto:contact@cigref.fr); Adresse : 21 avenue de messine 75008 Paris.
- Lien sur internet : <https://www.cigref.fr/wp/wp-content/uploads/2015/11/CIGREF-Economie-donnees-perso-Enjeux-business-ethique-2015.pdf>
- Projet Jourdain : Approche économique des données personnelles concernant le journalisme, information et Data présenté par Fabrice Rochelandet a l'université de la Sorbonne Paris 3 .La vidéo du séminaire est présente sur YouTube sur le lien suivant : <https://www.youtube.com/watch?v=ZdjW40-l82w>
- [www.Cnil.fr](http://www.Cnil.fr) : le site de la commission national de l'informatique et des libertés, nombreuses ressources sur les décisions et les rapports annuels de la CNIL, la législation française et des dossiers complets sur les thèmes d'actualité concernant le sujet.
- <https://www.village-justice.com/articles/protection-des-donnees-personnelles-quel-interet-pour-les-particuliers,28487.html>
- <https://www.cnil.fr/fr/le-reglement-europeen-sur-la-protection-des-donnees-en-dataviz>
- [http://www.globalcis.org/aiss/ppl/AISS%20vol.3%20no.9\\_31.pdf](http://www.globalcis.org/aiss/ppl/AISS%20vol.3%20no.9_31.pdf)
- Formulaire d'Engagement CNIL :  
<https://declarations.cnil.fr/declarations/declaration/declarant.display.action;jsessionid=708C05C76C7985C7CF6D02CCA883CB63>