Protection des données personnelles

Introduction :

Dans notre société actuelle, Internet a pris une place considérable et est devenu le vecteur principal d'information, de communication et d'échanges. Dès lors, nous partageons de plus en plus de données sur le web, en particulier nos données personnelles (dossiers, mails mais aussi coordonnées, photos, etc.). Cependant, il n'y a pas (ou très peu) de transparence quant à l'utilisation de ces données. Il est donc légitime de se demander ce que les grands sites du GAFA (Google, Apple, Facebook, Amazon) et autres font de ces données.

A l'aube de la promulgation de la loi sur le renseignement qui vise une légalisation de la surveillance de masse dans le cadre de la lutte antiterroriste, il est également nécessaire de bien comprendre le rôle de l'État dans la protection des données personnelles.

Le débat s'articulera autour de différentes problématiques : tout d'abord nous parlerons du rôle de l'état, puis de la protection mise en place par celui-ci. Nous évoquerons par la suite les problèmes de transparence et de marchandisation des données.

Protection des données personnelles

I. Le rôle de l'État dans la protection des données personnelles : entre surveillance et liberté

A. Internet : une technologie ambigue

L'apparition d'internet a permis une amélioration considérable de la communication, du partage et du flux des idées : tout ceci a créé une nouvelle société virtuelle dans laquelle tout le monde peut se réinventer une vie et s'identifier à de nouvelles communautés en permanence (notamment sur les réseaux sociaux). L'individu n'est alors plus assigné à une identité particulière, il est libre de choisir celle qui lui convient et d'en changer à son gré. Internet a donc accordé une nouvelle forme de liberté aux utilisateurs.

Cependant, si l'utilisateur a la possibilité de se créer une infinité de vies, il ne peux pas les supprimer complètement : internet est une technologie d'archivage, où toutes les informations sont sauvegardées et répertoriées. Tout le passé d'un individu est donc connu et accessible et des informations le concernant peuvent être utilisées contre lui : c'est ce caractère rétrospectif qui est utilisé par les gouvernements pour pouvoir surveiller les citoyens.

B. La nécessité d'un contrôle des données

L'État est garant de la protection de la vie privée d'un individu. Cela se traduit concrètement par la promulgation de lois visant cette protection, comme la loi Informatique et libertés ou le droit à l'oubli. L'État est également garant de notre liberté et de notre sécurité, il est donc nécessaire qu'il puisse avoir accès aux informations concernant un individu potentiellement dangereux pour pouvoir le surveiller. Notons qu'internet facilite grandement cette surveillance (grâce notamment à l'archivage des données) .

Prenons pour exemple le cyberterrorisme. Actuellement, les grands groupes terroristes (Daech, Boko Haram…) se servent d'internet comme un moyen de recrutement, en faisant de la propagande, de revendication mais aussi d'attaques (plusieurs cyberattaques visant des sites français ont eu lieu à la suite des attentats contre Charlie Hebdo et le compte twitter du Commandement américain a été piraté début janvier par un groupe qui se revendiquait de l'organisation de l'État islamique).

C. Les dérives potentielles de cette surveillance

Il parait donc légitime, voire nécessaire que l'État puisse avoir accès aux données personnelles des citoyens dans le cadre d'une surveillance. Cependant, ce contrôle peut s'avérer risqué et menace notre liberté. D'abord, parce qu'il est effectué dans le plus grand silence pour éviter tout soupçon des individus surveillés. De plus, comme l'a montré Edward Snowden en révélant que le gouvernement américain espionnait même ses alliés grâce à internet, la surveillance effectuée va au delà de la simple filature des individus menaçants. Par ailleurs, le projet européen Indect, qui vise la surveillance automatique sur

le Web des comportements suspects, s'inscrit parfaitement dans cet augmentation des contrôles et dans cette menace de la liberté individuelle.

L'État joue donc un rôle ambivalent entre protection de la liberté et contrôle permanent.

Jusqu'où peut-il aller dans la surveillance des citoyens? Quelle transparence l'État doit-il appliquer à ces contrôles? Comment les États peuvent-ils légiférer à un niveau mondialisé?

II. Les moyens mis en place pour protéger les données

A. La création de la CNIL et les autres lois

Dans le cadre de la protection des données personnelles des citoyens, le gouvernement français avait mis en place, en 1978, la loi «Informatique et libertés» qui, encore aujourd'hui, réglemente le fichage informatique des individus. Cette année fut également créée la CNIL (Commission nationale de l'informatique et des liberté), organisme chargé de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte pas atteinte aux libertés, aux droits de l'homme ou aux vies privées. L'un des principaux droits de cette loi est le «droit de rectification et de radiation» qui permet à toute personne de demander la modification ou la suppression de données détenues sur elle. Dans ce souci de contrôle des données personnelles par les individus eux-mêmes, le «droit à l'oubli» a été mis en place en Europe, le 13 mai 2014. Cette directive accorde aux citoyens européens le droit de demander le déréférencement des liens qui apparaissent suite à la recherche de leur nom sur un navigateur internet.

Cependant, les personnes demandant ce genre de requête sont en droit de se demander ce qu'il advient de leurs données une fois supprimées. De plus, à l'heure actuelle, les données sont stockées dans des Big Data où elles sont analysées et répertoriées par des algorithmes. Le suivi de la suppression des données est donc bien plus difficile que s'il n'était pas entièrement régi par des algorithmes.

B. Les problèmes de transparence

Les révélations d'Edward Snowden ont montré le grand manque de transparence de la part des États quant à la surveillance des individus. Mais ce manque de transparence est également flagrant pour les grands sites détenteurs de données personnelles. En effet, même s'il est désormais possible de demander un déréférencement, nous ne savons pas ce que font les sites avec les données supprimées.

Il est indispensable de savoir à quoi servent nos données et comment elles sont traitées, sans quoi nous risquons de perdre notre liberté face aux États et aux sites internet. Prenons l'exemple de Hilary Clinton qui utilisait sa messagerie personnelle pour envoyer des emails de nature professionnelle. Elle a sans doute fait cela pour échapper à

la surveillance des échanges et ainsi jouir d'une plus grande liberté mais cela empêche des investigations nécessaires (Cf. partie 1).

Quelle solution adopter afin de protéger ses données personnelles?
A quel niveau la CNIL peut-elle intervenir?
La transparence est elle possible ou illusoire?

III. Le problème de la marchandisation des données

A. La marchandisation des données

Nos informations ont une valeur marchande pour les acteurs de l'internet. Certaines entreprises rachètent nos données aux sites afin de proposer des services personnalisés et de réutiliser ces données pour une utilisation performante de ces services. À l'heure actuelle, nous estimons que 85% des données personnelles sont détenues par des grandes entreprises.

Ce stockage et ce marché de données présente, à première vue, une simplification d'internet : en proposant des services personnalisés, les entreprises permettent alors à l'utilisateurs de s'affranchir de choix et de décisions triviales. De plus, les sites faisant du profit sur la revente d'informations peuvent alors proposer des services gratuits qui facilitent là aussi la vie de l'utilisateur.

B. Les risques de cette marchandisation

Cependant, en demandant à des algorithmes de faire des choix à notre place, nous perdons peu à peu notre capacité de décision et par conséquent, nous perdons notre liberté individuelle.

Nos données sont également vendues à des fins marketing. Les sites publicitaires peuvent aux aussi acheter nos informations, et le site principal nous propose alors de la publicité ciblée. À titre d'exemple, Facebook (qui possède 1,393 milliards d'utilisateurs) a réalisé un bénéfice de 2,94 milliards de dollars dont 90% viennent de la publicité ciblée. L'individu n'est alors plus considéré comme une personne mais comme une cible marketing. Par ailleurs, profitant d'un service gratuit, il ne perçoit pas cette mercantilisation et est donc exclu volontairement d'un problème, qui le concerne au plus haut point : la marchandisation de sa vie privée.

Comment limiter la marchandisation de nos données? Quelle valeur donner à nos information personnelles? Y a-t-il une loi du marché de données?