Introduction à la confidentialité sur l'Internet

Fiche de l'Internet Society sur les politiques publiques

La confidentialité contribue à renforcer la confiance des utilisateurs dans les services en ligne. Cependant le respect de la confidentialité en ligne est sans arrêt menacé. Promouvoir des lois fortes, neutres technologiquement permettant d'encadrer la confidentialité des données, des principes de confidentialité dès la création de ces dernières, une éthique de collecte des données et des principes de traitement de ces dernières constitue une approche clé pour promouvoir la confidentialité en ligne.

Introduction

Le respect de la confidentialité est un droit important [1]et un catalyseur essentiel de l'autonomie, de la dignité et de la liberté d'expression d'un individu. Pourtant, il n'y a pas de définition universellement acceptée de la confidentialité. Dans le contexte de l'Internet cependant, une compréhension commune de la confidentialité est *le droit de déterminer quand, comment et dans quelle mesure les données personnelles peuvent être partagées avec d'autres.*

Dans l'ère numérique d'aujourd'hui, la collecte d'informations est rapide, facile et moins chère que jamais. Les progrès sur une variété de fronts technologiques ont contribué à ce nouveau monde. Par exemple :

- Le stockage des données n'est pas cher, rendant les données accessibles en ligne pendant de longues périodes de temps.
- Le partage de données peut être rapide et distribué, permettant aux données de proliférer facilement.
- Les outils de recherche sur Internet peuvent reconnaître des images, des visages, des sons, la voix et suivre les déplacements, ce qui facilite le suivi des appareils et des individus qui sont connectées au fil du temps et partout.
- Des outils sophistiqués sont développés pour relier, corréler et regrouper des données apparemment sans rapport à grande échelle.
- Il devient de plus en plus facile d'identifier les individus - et les classes d'individus - à partir de données prétendument anonymes ou rendues anonymes.
- Il y a de plus en plus de capteurs dans les objets et appareils mobiles connectés à l'Internet.

Les données personnelles sont devenues une marchandise rentable. Chaque jour, les utilisateurs partagent plus de données personnelles en ligne, souvent à leur insu, et l'Internet des objets va démultiplier encore

[1]Voir laDéclaration Universelle des droits de l'Homme de l'ONU, *http://www.un.org/en/documents/udhr/*; Pacte international relatif aux droits civils et politiques: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx, *et la* Convention européenne des droits de l'Homme, *http://www.echr.coe.int/Documents/Convention_ENG.pdf*.

plus cela. Ces facteurs ont le potentiel d'exposer des données personnelles et de créer des problèmes de confidentialité sur une plus grande échelle que jamais auparavant.

Dans cet esprit, il est important d'encourager le développement et l'application de cadres de confidentialité qui appliquent une approche éthique à la collecte et à la gestion des données. Les cadres qui intègrent, entre autres, les concepts d'équité, de transparence, de participation, de responsabilité et de légitimité.

Considérations clés

Bien qu'il n'y ait pas de loi universelle sur la confidentialité ou sur la protection des données qui s'applique sur l'Internet, un certain nombre de cadres internationaux et nationaux sur confidentialité ont largement convergé pour former un ensemble de principes de base sur la confidentialité. Les principes suivants sont tirés des *Directives sur la confidentialité de 2013* rédigés par l'Organisation pour la coopération et le développement économiques (OCDE) et sont largement reconnus comme fournissant une bonne base pour l'élaboration de politiques et pratiques de protection des informations personnelles en ligne :

- **Limitation du recueil des données.** Il devrait exister des limites à la collecte de données personnelles. Toutes ces données devraient être obtenues par des moyens légaux et équitables et, le cas échéant, avec la connaissance ou le consentement de la personne concernée.
- **Qualité des données.** Les données personnelles doivent être pertinentes aux fins pour lesquelles elles doivent être utilisés, et, dans la mesure nécessaire à ces fins, elles devraient être exactes, complètes et mises à jour.
- **Spécification de l'objectif.** Les finalités pour lesquelles les données personnelles sont recueillies doivent être précisées. L'utilisation doit être limitée à ces fins ou à d'autres fins qui ne sont pas incompatibles.
- **Limitation de l'utilisation.** Les données personnelles ne doivent pas être divulguées, mises à disposition ou utilisées à d'autres fins, sauf consentement de la personne ou si la loi l'autorise.
- **Les mesures de sécurité.** Les données personnelles doivent être protégées par des mesures de sécurité raisonnables.
- **Ouverture.** Il devrait y avoir une politique générale de transparence des développements, des pratiques et des politiques en matière de données personnelles.
- **Participation individuelle.** Les individus devraient avoir le droit d'obtenir des informations sur les données personnelles détenues par d'autres et avoir le droit de les effacer, rectifier, compléter ou de les modifier, le cas échéant.
- **Responsabilité.** Ceux qui recueillent des données personnelles devraient être tenus pour responsables du respect de ces principes.

Il convient de noter que beaucoup de ces principes impliquent la transparence en ce qui concerne qui recueille les données, et l'utilisation qui en est faite.

Défis

Les décideurs politiques doivent tenir compte d'un certain nombre de défis clés pour déterminer les actions liées à la confidentialité en ligne. Certains défis largement reconnus comprennent :

1. **Déterminer quelles données doivent être protégées.** Typiquement, les lois sur la protection des données et la confidentialité s'appliquent aux données personnelles, aussi connues comme sous les

termes *informations personnelles ou renseignements personnels* dans certaines juridictions. Une définition commune des données personnelles est la suivante : « toute information concernant une personne physique identifiée ou identifiable ». [2]Toutes les définitions ne sont pas les mêmes. En outre, il peut être difficile de déterminer quelles données spécifiques doivent être considérées comme des renseignements personnels dans un contexte particulier. L'évolution rapide des services, ainsi que la technologie utilisée pour traiter les données, font que déterminer ce qui devrait être protégé devient un défi permanent.

2 **Exigences juridiques de protection des données différentes.** Les lois sur la confidentialité ne sont pas les mêmes dans tous les pays. Cela signifie que certaines données peuvent être protégées par la loi dans un pays, mais pas dans un autre. En outre, même lorsque les données sont couvertes par les lois des deux pays, les protections peuvent varier (par exemple, la collecte de données peut être faite sur l'accord de la personne concernée (opt-in) ou par défaut sauf si la personne concernée ne donne pas son accord (opt-out). Pour compliquer encore les choses, plus d'un pays peut faire valoir que ses lois sont applicables. Par exemple, un pays peut faire valoir que ses lois sur la protection des données s'appliquent parce que les données personnelles concernent ses citoyens, tandis qu'un autre peut affirmer que sa loi s'applique parce que la société recueillant les données est basée sur son territoire. Donner effet aux droits et aux attentes de confidentialité de l'individu peut être particulièrement problématique lorsque les lois des pays sont en conflit direct ou incompatibles. En particulier, les récentes controverses relatives à la surveillance de masse ont soulevé la question de savoir si les clauses « nécessaires et proportionnées » dans la législation fournissent une protection suffisante pour les citoyens. Les débats internationaux sur la surveillance soulignent combien il est difficile pour les États-nations de se mettent d'accord sur l'interprétation cohérente des conventions internationales dans le domaine de la confidentialité, comme sur les droits de l'Homme, ou les droits civils et politiques.

3 **Protéger la confidentialité lorsque les données traversent les frontières.** L'Internet dépasse les frontières nationales, mais les lois sur la confidentialité et la protection des données sont basées sur la souveraineté nationale. Par conséquent, des dispositions spéciales sont nécessaires pour protéger les données à caractère personnel qui quittent un pays et entrent dans un autre, afin d'assurer la continuité de la protection des données pour les utilisateurs. Les approches varient, mais ont tendance à faire attention quant à savoir si le pays d'accueil dispose d'une protection « adéquate ». Divers cadres ont vu le jour pour faciliter les flux transfrontaliers de données au sein d'une région ou entre régions.[3]

4 **Consentement réellement significatif.** Les lois sur la confidentialité et la protection des données permettent généralement un certain degré de collecte et d'utilisation des données personnelles si la personne donne son consentement. En théorie, cette approche permet aux internautes d'avoir un certain niveau de contrôle ou de choisir la manière dont leurs données sont collectées et utilisées par autrui. Cependant, dans la pratique, les utilisateurs de services en ligne ne peuvent pas lire ou ne peuvent pas comprendre ce à quoi ils consentent (par exemple, parce que les conditions générales d'utilisation sont

[2]; Pour consulter les définitions relatives aux données personnelles, voir : *Directives mises à jour en 2013 sur la confidentialité de l'OCDE, La Convention 108 du Conseil de l'Europe ; La Directive sur la protection des données de l'UE (1995) et la Convention de l'Union africaine sur la cyber sécurité et la protection des données personnelles*

[3]*Exemples de cadres transfrontaliers : APEC Cross Border Privacy Rules (CBPR) system, US-EU Safe Harbor Framework, EU Binding Corporate Rules.*

longues et rédigées dans un langage juridique complexe). Même s'ils en comprennent les termes, les utilisateurs peuvent être incapables de les négocier. L'utilisation généralisée des appareils mobiles avec des capteurs et de petits écrans sur lesquels on affiche les options de confidentialité, et les utilisations secondaires fréquents de données personnelles (par exemple, la publicité ciblée) créent des difficultés supplémentaires aux utilisateurs pour qu'ils exercent un contrôle sur leurs données personnelles. Une approche technique pourrait être d'encourager le développement de systèmes qui font qu'il serait plus facile pour l'utilisateur de comprendre et de gérer les informations qui sont collectées par les appareils connectés intelligents qui les entourent.

Principes directeurs

Comme les données personnelles ont une valeur monétaire et stratégique pour autrui, c'est un défi de s'assurer qu'elles sont seulement recueillies et utilisées de manière appropriée. Les principes directeurs suivants favorisent la réalisation de cet objectif :

- **Interopérabilité mondiale.** Encourager les normes de confidentialité ouvertement développées et interopérables au niveau mondial (à la fois au niveau technique et réglementaire) qui facilitent les flux de données transfrontaliers, tout en protégeant la confidentialité.
- **Collaboration.** Encourager la collaboration multipartite et une approche holistique qui garantit de la valeur à toutes les parties prenantes.
- **Déontologie.** Encourager les cadres de confidentialité qui appliquent une approche éthique de la collecte de données et de leur gestion. Les approches éthiques intègrent, entre autres choses, les concepts d'équité, la transparence, la participation, la responsabilité et la légitimité dans la collecte et le traitement des données.
- **Impact de la confidentialité.** Comprendre l'impact de la confidentialité de la collecte et de l'utilisation des données personnelles. Prendre en considération les implications de confidentialité des métadonnées. Reconnaître que même la simple possibilité de la collecte de données à caractère personnel pourrait interférer avec le droit à la confidentialité. En outre, comprendre que la confidentialité d'une personne peut être touchée, même si elle n'est pas identifiable, mais qu'elle peut juste être isolée.
- **Anonymité et pseudo-anonymité.** Les individus doivent avoir la capacité de communiquer de façon confidentielle et anonyme sur Internet.
- **Minimisation des données.** Encourager les pratiques de minimisation des données. Insister sur la collecte et l'utilisation sélectives des seules données nécessaires pour le temps nécessaire.
- **Choix**. Donner aux utilisateurs la possibilité de négocier la collecte des données et les modalités de leur gestion justes, sur un pied d'égalité avec les collecteurs de données, ainsi que de pouvoir donner un consentement significatif.
- **Environnement juridique.** Promouvoir des lois fortes et neutres technologiquement, leur respect et leur application effectifs. Ces lois devraient se concentrer sur les résultats souhaités en matière de confidentialité plutôt que de préciser des moyens technologiques particuliers pour orienter les pratiques de confidentialité.
- **Environnement technique.** Encourager des environnements ouverts qui soutiennent le développement volontaire fondé sur le consensus des protocoles et des normes qui prennent en charge des solutions améliorées de confidentialité.

- **Environnement d'affaires.** Encourager les entreprises à reconnaître que les approches respectant la confidentialité peuvent fournir des avantages concurrentiels et peuvent réduire leur exposition aux risques juridiques.
- **Principes de confidentialité dès la conception.** Promouvoir la confidentialité dès la conception et tout au long du cycle de développement, de la mise en œuvre et du déploiement. Les principes de confidentialité dès la conception devraient également être appliqués à l'élaboration des normes, des applications, des services et des processus commerciaux.
- **Outils.** Promouvoir le développement d'outils utilisables qui permettent aux utilisateurs d'exprimer leurs préférences de confidentialité et de communiquer en toute confidentialité (par exemple, le cryptage) et de façon anonyme ou sous un pseudonyme ; et permettre aux fournisseurs de services d'offrir des choix et une visibilité sur ce qui se passe avec les données de l'utilisateur.

Ressources supplémentaires

L'Internet Society a publié plusieurs articles et du contenu supplémentaire en rapport avec cette question. Ils sont librement accessibles sur le site Web de l'Internet Society.

- Page de ressources de l'Internet Society sur la confidentialité, http://www.internetsociety.org/our-work-privacy.
- Ressources de l'Internet Society sur l'empreinte numérique, http://www.internetsociety.org/your-digital-footprint.
- Comprendre votre identité en ligne : aperçu sur l'identité, http://www.internetsociety.org/understanding-your-online-identity-overview-identity.
- Comprendre votre identité en ligne : protection de votre confidentialité , http://www.internetsociety.org/understanding-your-online-identity-protecting-your-privacy.
- Comprendre votre identité en ligne : apprendre à protéger votre identité en ligne , http://www.internetsociety.org/understanding-your-online-identity-learning-protect-your-identity.

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Genève, Suisse
Tél : +41 22 807 1444 • Fax : +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave., Suite 201
Reston, VA 20190 USA
Tél : +1 703 439 2120 • Fax : +1 703 326 9881
E-mail : info@isoc.org

bp-privacy-20151030-fr