Comité: Union Internationale des Télécommunications
Problématique: Définir des normes internationales, orientées vers le futur, pour le droit à la vie privée en ligne
Présidents: Charles Hermann Gomez, Antonio Badilla Olivas, Marit Pauwelyn

Définir des normes internationales, orientées vers le futur, pour le droit à la vie privée en ligne

Les TIC pour les ODD:

L'Union Internationale des Télécommunications est une organisation de l'ONU qui a pour mission de standardiser, harmoniser et réguler le développement des technologies de l'information et de la communication (TIC, ou ICTs en anglais) au niveau mondial. Un de ses objectifs est de promouvoir l'inclusivité et l'accès universel à ces technologies. L'UIT collabore aussi avec d'autres organisations de l'ONU afin d'exploiter de manière efficace le potentiel des TIC pour réaliser les objectifs du développement durable (ODD, ou SDGs).

Introduction

Nous vivons dans un monde où tout est en ligne. On pourrait même dire, nous vivons en ligne. Toutes nos conversations, recherches, idées, expériences, opinions, amis, photos, chansons que nous écoutons dans le bus, chaque information qui nous concerne est absorbée par cet espace incroyablement complexe qu'est l'Internet. Cet espace étant désormais accessible presque au monde entier, le droit d'un individu à la vie privée est en jeu à tout moment. Celui-ci affecte la capacité d'exercer presque tous les autres droits, en particulier la liberté d'expression et la liberté de réunion et d'association. Mais la vie privée en ligne ne nous concerne pas qu'individuellement, il s'agit de savoir comment notre gouvernement, mais également d'autres organisations et associations, utilisent nos informations dans leur intérêt. En effet, les gouvernements ont renforcé leur capacité à surveiller les mouvements de citoyens, à censurer les discours, à bloquer ou à filtrer l'accès à l'information et à suivre les communications afin de contrôler nos informations et nos opinions sociales, économiques et politiques sur le monde. Alors jusqu'où cela ira-t-il? Jusqu'où vivrons-nous dans un monde où nous n'avons bientôt plus le droit d'être un simple individu? Comment pouvons-nous, en tant qu'Union Internationale des Télécommunications, empêcher que cela aille trop loin?

Mots-clés

Le droit à la vie privée, comment le définir universellement?

Il est sans doute important de partir de la base du droit fondamental à la vie privée qui a été déclaré dans l'Article 12 de la Déclaration Universelle des Droits de l'Homme:

"Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation."

De tous les droits de l'homme, la vie privée est peut-être le plus difficile à définir et à circonscrire. Les définitions de la vie privée varient considérablement selon le contexte et l'environnement. Dans de nombreux pays, le concept a été fusionné avec la protection des données, qui interprète la vie privée en termes de gestion des informations personnelles. En dehors de ce contexte plutôt strict, la protection de la vie privée est souvent considérée comme un moyen de déterminer à quel point la société peut s'immiscer dans les affaires d'une personne. Elle est souvent divisé en quatre catégories:

- La confidentialité des informations, qui implique l'établissement de règles régissant la collecte et le traitement de données à caractère personnel, telles que les informations de crédit et les dossiers médicaux;
- La protection de la vie privée, qui concerne la protection de la personne physique contre des procédures invasives telles que le dépistage de drogues et les fouilles caverniculaires;
- Confidentialité des communications, qui couvre la sécurité et la confidentialité du courrier, des téléphones, des courriers électroniques et d'autres formes de communication; et
- La vie privée territoriale, qui concerne la fixation de limites à l'intrusion dans les environnements domestiques et autres, tels que les lieux de travail ou les espaces publics.

Presque tous les pays du monde reconnaissent explicitement le droit à la vie privée dans leur Constitution. Au minimum, ces dispositions incluent les droits d'inviolabilité du domicile et de confidentialité des communications. Les constitutions les plus récentes, telles que celles de l'Afrique du Sud et de la Hongrie, incluent des droits spécifiques d'accès et de contrôle des informations personnelles.

Dans de nombreux pays où la vie privée n'est pas explicitement reconnue dans la Constitution, tels que les États-Unis, l'Irlande et l'Inde, les tribunaux ont jugé ce droit garanti par d'autres dispositions. Dans de nombreux pays, des accords internationaux reconnaissant le droit à la vie privée, tels que le Pacte international relatif aux droits civils et politiques ou la Convention européenne des droits de l'homme, ont été adoptés.

Plus spécifiquement, quelle est le droit à la vie privée en ligne?

La confidentialité sur Internet, également appelée confidentialité en ligne, est un sous-ensemble de la confidentialité des données et un droit humain fondamental. En effet, il fait référence à la vie privée à laquelle un individu a droit lorsqu'il affiche, stocke ou fournit des informations sur

lui-même sur Internet. Cela peut inclure à la fois des informations d'identification personnelle (IIP) et des informations d'identification non personnelles (IINP), telles que son comportement sur un site Web. Sans la confidentialité sur Internet, toutes ses activités sont susceptibles d'être rassemblées et analysées par quelconques parties intéressées!

Qu'est-ce qu'une donnée personnelle ?

Il s'agit de toutes informations se rapportant à une personne physique identifiée ou identifiable, directement ou non, grâce à un identifiant ou à un ou plusieurs éléments propres à son identité.

Il peut s'agir par exemple d'un nom, d'un prénom, d'une adresse électronique, d'une localisation, d'un numéro de carte d'identité, d'une adresse IP, d'une photo, d'un profil social ou culturel.

Finalement, qu'est ce qu'une norme internationale?

Pendant les débats, il faudra en effet définir des normes internationales concernant le sujet, c'est à dire des résolutions qui aident chaque délégation et dont les solutions sont accessibles et faisables pour tous. C'est pour cela qu'elles seront internationales.

Apercu général

La situation et les enjeux actuelles

- ➔ **Ou sont stockés les données personnelles?**

Les outils en ligne
Les outils en ligne ont la capacité de suivre et de stocker la localisation, la consommation d'informations, les habitudes d'achat, les interactions sociales, et même, via les assistants personnels numériques, le comportement et les discussions domestiques de leurs utilisateurs. Voici quelques outils importants qui nous entourent quotidiennement:

1. **Les réseaux sociaux (IIP)**

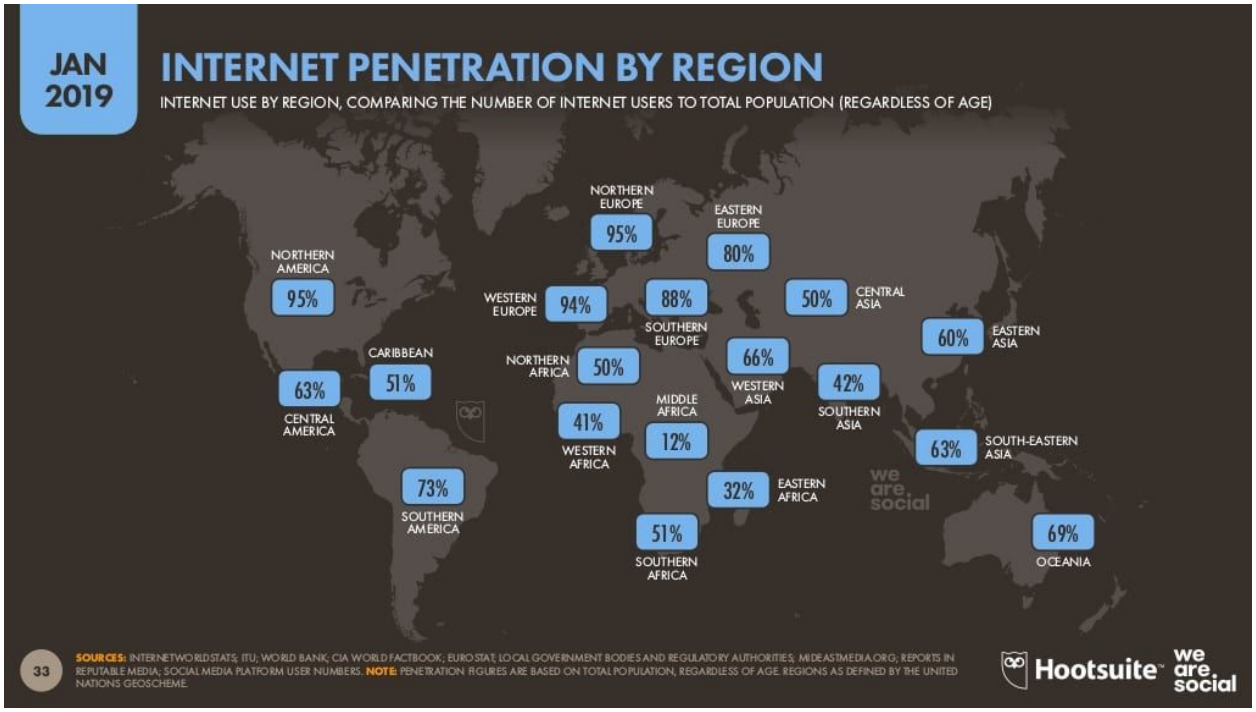
L'utilisation naïve des réseaux sociaux peut engendrer des conséquences émotionnelles, financières mais aussi juridiques et mener, dans certains cas, à la divulgation ou propagation de données personnelles. Les enfants et adolescents courent déjà un risque sur les réseaux sociaux, mais les adultes, les pouvoir publics, les banques et même les grandes entreprises Web ne sont eux aussi pas à l'abri des risques.

Les réseaux sociaux sont plus populaires que jamais. Sur les quelques 3,43 milliards d'utilisateurs Internet dans le monde, 2,28 milliards de personnes (donc environ presque un tiers de la population mondiale) visitent régulièrement les réseaux sociaux (une tendance en

hausse). Plateforme qui enregistre le plus grand nombre de clics mensuels, Facebook est en tête du peloton et célèbre une double victoire parmi les utilisateurs d'appareils mobiles avec sa filiale WhatsApp.

L'utilisateur n'est pas seulement consommateur, il est aussi acteur, il crée du contenu (textes, vidéos, photos,…) à la différence de l'internet traditionnel. En effet, derrière chaque réseau social, il y a des personnes qui ont accès à toutes vos données, mêmes celles dites "privées". Sur internet, on ne peut rien contrôler.

Les réseaux sociaux sont remplis de pirates, cybercriminels et vendeurs de données. Lorsqu'on regarde cette carte, on peut voir que l'internet est présent à travers le monde, dans certains pays plus que dans d'autres. Cela veut aussi dire que les réseaux sociaux occupent une place importante dans le monde entier, mettant plus de la moitié de la population globale à risque dans ce qui concerne l'invasion de la vie privée.

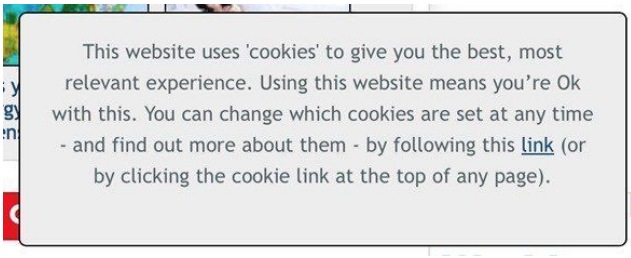


(https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/)

2. L'utilisation des cookies (IINP)

Les cookies ou aussi appelés les témoins de connexion, existent depuis plus de 20 ans sur internet. Ils permettent de conserver des données utilisateurs au cours d'une connexion, dans le but de faciliter la navigation aux internautes. Ils ont différentes fonctions notamment dans le cas d'une activité e-commerce pour stocker le contenu d'un panier d'achat, pour enregistrer les

paramètres de langue d'un site internet, ou dans une visée plus commerciale, pour faire de la publicité ciblée. Cependant, les cookies ont toujours été plus ou moins controversés car ces fichiers textes contiennent des informations personnelles qui peuvent potentiellement être exploitées par des tiers, pouvant entraîner un risque en termes de sécurité.



Il existe un règlement pour sécuriser la vie privée de l'internaute, qui insiste sur le consentement de l'individu avant le dépôt de cookies, la communication sur la finalité de ces cookies et un moyen de s'y opposer. De plus, ce consentement est valide pendant maximum 13 mois. (https://www.termsfeed.com/blog/4-ways-notify-users-cookies/)

Toutefois, il existe beaucoup de dangers et de risques en acceptant ces cookies. En effet, ils facilitent le travail des hackers, l'objectif étant pour eux d'en exploiter le contenu et d'utiliser ces données personnelles à des fins malveillantes pouvant aller jusqu'à la mise en place des cyberattaques. Par exemple, la NSA (National Security Agency) utilise ces cookies pour surveiller la vie des internautes, comme le dévoilent les documents publiés en décembre 2013 par Edward Snowden. Selon le *Washington Post*, la technique utilisée par la NSA et la GCHQ, l'agence de renseignement britannique, consiste à se procurer des cookies PREF, propres à Google, afin d'identifier les cibles et surveiller leur navigation. Au nom de la protection nationale et sous couvert du « Patriot Act », cet ensemble de lois qui contraint les entreprises américaines à fournir les informations désirées, la NSA s'est octroyé le droit d'accès à ces informations.

3. Les assistants personnels numériques (IINP)

Majoritairement présents dans les smartphones, ces outils, plus connus sous les noms de Siri, Alexa, Google Assistants ou encore Cortana, sont souvent cachés dans une enceinte et servent d'assistant domestique. Grâce à leur intelligence artificielle, ils répondent aux questions ou ordres de leur propriétaire après avoir entendu l'appel spécifique attendu par la machine.
(image: film HER, traitant une relation amoureuse entre un homme et une assistante personnelle:http://www.allocine.fr/film/fichefilm-206799/dvd-blu-ray/?cproduct=374684)

De plus en plus de doutes se posent concernant l'intention de ces "assistants", beaucoup de théories se sont formés disant qu'ils sont très dangereux et risquent de faire beaucoup plus que seulement réagir aux attentes des humains. En principe, ces appareils se déclenchent

lorsque l'utilisateur prononce le mot-clé attendu ("Alexa", "OK Google" etc.). Avant ce mot-clé, ils "écoutent", mais n'envoient en principe aucune information sur le réseau. Après le mot-clé, les conversations sont envoyées dans le "cloud" afin de traiter la commande. Amazon, Google ou Apple assurent que les données sont chiffrées et qu'il n'y pas d'écoute sauvage. Quoi qu'en disent les entreprises, *"derrière les assistants vocaux, des humains vous entendent",* prévient *La Quadrature du Net,* qui défend les libertés dans l'univers numérique. Des êtres humains aident en effet les machines à devenir intelligentes en écoutant et en vérifiant les retranscriptions de propos tenus. Les assistants personnels, ne seraient-ils pas que des aides domestiques mais des espions du gouvernement? Il y a eu de nombreux incidents qui semblent justifier ces idées, mais les créateurs semblent toujours trouver une explication. Cette invention, surpasse t-elle les limites de la vie privée de l'individu? Qui pourrait décider de ces règlements?

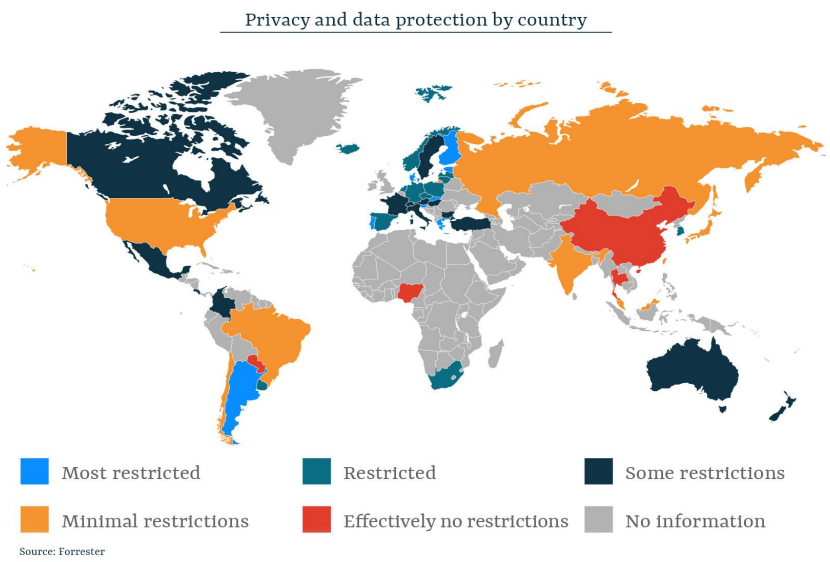
- ➔ **Quelles sont les lois instaurés pour limiter l'utilisation de ces données personnelles?**

Comme indiqué précédemment dans le rapport, presque tous les pays reconnaissent le droit à la vie privée et la protègent par le biais de leurs lois. Mais quel cadre législatif a été établi au niveau international?

Dans le monde entier, un mouvement général en faveur de l'adoption de lois qui s'appuie pour la plupart sur les modèles mis en place par l'Organisation de Coopération et de Développement Economiques (https://www.oecd.org/fr/) et le Conseil de l'Europe (https://www.coe.int/fr/) est en cours.

En 1995, consciente à la fois des lacunes du droit et des nombreuses différences de niveau de protection dans chacun de ses États, l'Union Européenne a adopté une directive européenne qui offre aux citoyens une protection plus variée et détaillée contre les utilisations abusives de leurs données.

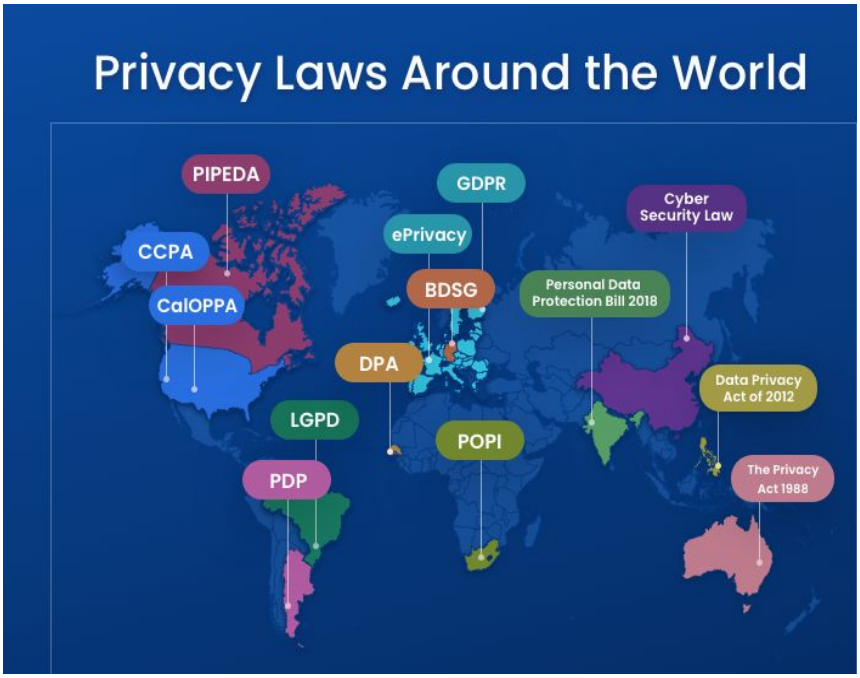
La directive impose aux États membres de veiller à ce que les données personnelles relatives aux citoyens européens soient couvertes par la loi lorsqu'elles sont exportées vers, ou traitées dans, des pays en dehors de l'Europe. Cette exigence a entraîné une pression croissante sur les autres gouvernements, menant à que plus de quarante autres pays instaurent des lois sur la protection des données ou la confidentialité des informations. D'autres sont en cours d'adoption.



Pourquoi adopter des lois exhaustives?

- **Pour remédier aux injustices passées**. De nombreux pays, notamment en Europe centrale, en Amérique du Sud et en Afrique du Sud, adoptent des lois pour corriger les atteintes à la vie privée commises sous les régimes autoritaires précédents.
- **Promouvoir le commerce électronique**. Beaucoup de pays comme par exemple ceux en Asie, mais aussi au Canada, ont élaboré ou sont en train d'élaborer des lois dans le but de promouvoir le commerce électronique. Ces pays reconnaissent que les consommateurs sont mal à l'aise avec l'envoi de leurs informations personnelles dans le monde entier. Les lois sur la protection de la vie privée font partie d'un ensemble de lois visant à faciliter le commerce électronique en établissant des règles uniformes.
- **S'assurer que les lois sont compatibles avec les lois paneuropéennes**. La plupart des pays d'Europe Centrale et Orientale adoptent de nouvelles lois fondées sur la Convention du Conseil de l'Europe et la directive de l'Union Européenne sur la protection des données. Certains espèrent rejoindre l'Union Européenne dans un avenir proche, d'autres, comme le Canada, adoptent de nouvelles lois pour garantir que le commerce ne sera pas affecté par les exigences de la directive de l'UE.

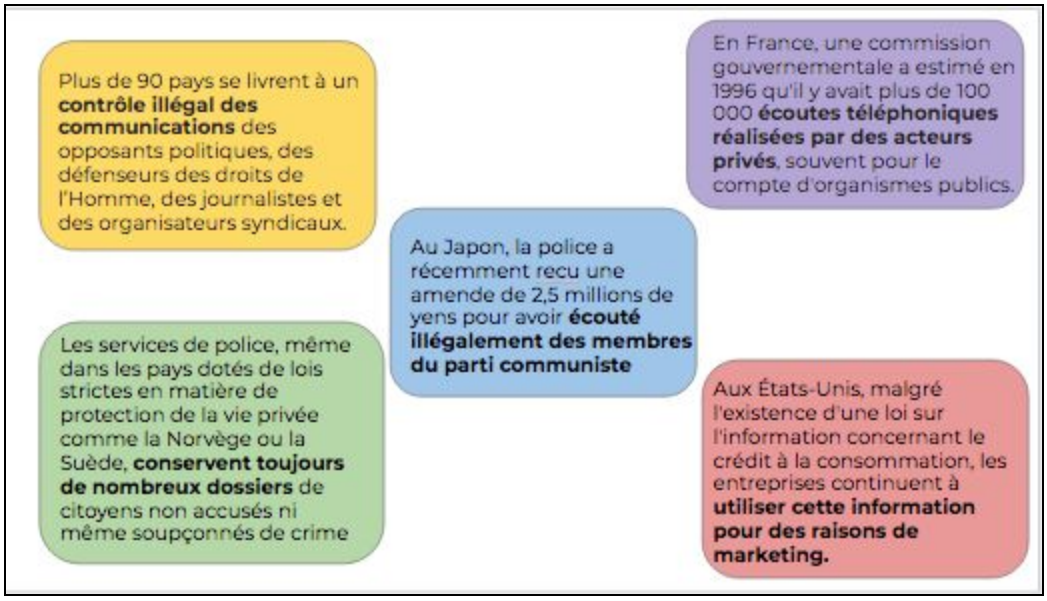
(http://gilc.org/privacy/survey/intro.html)



➔ **Quelles sont les enjeux de ces lois?**

- Le **développement intense de la technologie**, qui introduit de plus en plus de machines pouvant collecter, analyser et disséminer des données à une vitesse incroyable, crée beaucoup de confusions et de lacunes dans les lois de protection, et crée aussi proportionnellement plus de potentiel d'invasion de la vie privée. Avec cette croissance, la situation urgente ne fait que s'aggraver.
- De nouveaux développements en matière de recherche et de soins médicaux, de télécommunications, de systèmes de transport avancés et de transferts financiers ont considérablement accru le niveau d'informations généré par chaque individu.
- La **globalisation** supprime les limitations géographiques au flux de données. Le développement de l'Internet est peut-être l'exemple le plus connu d'une technologie globalisée.
- La convergence, dû au développement de la technologie, conduit à l'élimination des barrières technologiques entre les systèmes. Les systèmes d'information modernes sont de plus en plus interopérables avec d'autres systèmes et peuvent échanger et traiter différentes formes de données.
- Dans certains pays, les agences et les associations ont eu beaucoup d'exemption concernant l'application des lois de confidentialité

- Sans surveillance et mise en vigueur, **les lois sont parfois simplement ignorées**.



L'impact de l'atteinte à la vie privée sur la population

Il a toujours été difficile de définir quel impact résulte d'une violation de la vie privée d'un individu. Quelle est la différence entre quelqu'un qui entre chez vous sans autorisation ou à l'État qui écoute une conversation téléphonique personnelle? Il est de plus en plus difficile de répondre à cette question maintenant que les initiatives de collecte et de traitement de données se sont développées et ne sont plus axées que sur des individus spécifiques, mais sur la société dans son ensemble. Que fait-on de mal en collectant des données sur toute une population ou en enregistrant avec des caméras de surveillance la vie quotidienne des citoyens au coin de presque toutes les rues? Comment peut on prendre en compte ces préjudices sans preuves matérielles ou quantités spécifiques?

Quand un individu est en ligne, il devient énormément vulnérable en s'exposant à de nombreux risques et incertitudes: qui pourrait utiliser ses informations, pour quoi, et pour combien de temps? Respecter la vie privée c'est respecter les normes de quelles informations sont prises en compte, comment elles sont utilisées et avec qui elles sont partagées.

Dans cette ère technologique, la notion de préjudice devient de plus en plus problématique. Souvent, un individu est simplement inconscient que ses données personnelles sont utilisées par des citoyens (les réseaux sociaux), des entreprises (l'utilisation des cookies), ou par le gouvernement (la surveillance, par exemple des caméras). Si un individu va au tribunal pour défendre ses droits, comment pourrait il accuser qui que ce soit? Quel préjudice concret l'Agence de la Sécurité Nationale (NSA) a-t-elle fait sur un américain ou un citoyen quelconque?

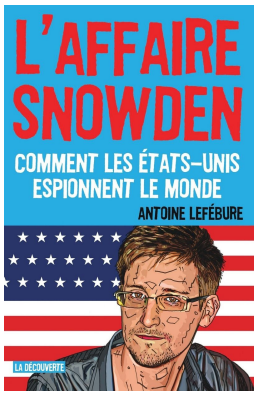
Les tribunaux ont beaucoup lutté contre ce problème de préjudice, et peu de progrès ont été fait. Nous avons désespérément besoin d'une meilleure compréhension et approche de ces violations.

Voici quelques exemples de ses impacts sur la population:

- L'exposition de leurs données leur a causé une détresse émotionnelle.
- L'exposition de leurs données les a exposées à un risque accru de préjudice lié au vol d'identité, à la fraude ou à toute autre blessure.
- L'exposition de leurs données les a obligés à dépenser du temps et de l'argent afin d'éviter de futures fraudes, telles que s'inscrire à la surveillance du crédit, contacter des agences d'évaluation du crédit, placer des alertes de fraude sur leurs comptes, etc.
- La collection ou l'utilisation de données sans consentement ou sans leur savoir

Les tribunaux n'acceptent souvent pas ces arguments car il n'y a pas de preuve valide, ou l'explication semble être trop personnelle et abstraite. Ces impacts sont donc dans la plupart des pays complètement ignorés.

Etudes de cas spécifiques



L'affaire Snowden

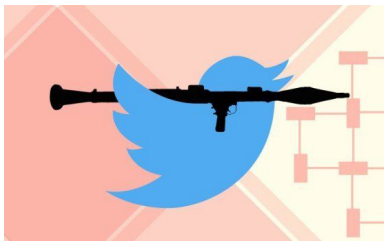
De Wikileaks aux «Paradise Papers», la dernière décennie a été marquée par une multiplication des révélations issues de fuites d'envergure de documents confidentiels. L'affaire Snowden, éclatée en 2013, concerne Edward Snowden, analyste de sécurité pour un sous-traitant de la NSA mais surtout le plus grand hackeur de son temps, qui a fuité des dizaines de milliers de documents de la NSA décrivant le programme de surveillance massif de l'agence américaine. Voici quelques révélations:

- plusieurs programmes de surveillance de masse, des appels téléphoniques et des échanges en ligne mis en place par la NSA.
- L'agence américaine s'est permis de mettre sur écoute de nombreux dirigeants étrangers. (par exemple les 3 derniers présidents français)
- De nombreuses données sont collectées sur les citoyens ordinaires aux Etats-Unis.
- La NSA fait évidemment de la surveillance dans un but antiterroriste mais verse aussi dans l'espionnage économique et industriel.

Après ces révélations, il y eut un choc non seulement pour les américains, mais pour le monde entier. Cet évènement était en quelques sortes un symbole du début de cette ère technologique ou toutes les données sont supervisées et enregistrées.

(http://www.leparisien.fr/international/tout-comprendre-a-l-affaire-snowden-07-11-2017-7378926.php)

La fameuse branche “cyber-djihadiste”



L’utilisation d’Internet à des fins terroristes est un phénomène en plein essor.

Internet peut être utilisé non seulement pour publier de la rhétorique et des vidéos extrémistes, mais également pour créer des relations avec les personnes les plus réceptives à la propagande, et solliciter leur soutien.

Les organisations terroristes ont de plus en plus recours à la propagande diffusée sur des plateformes comme les sites Web protégés par mot de passe ou les groupes de discussion à accès restreint pour recruter clandestinement. La portée d’Internet offre aux organisations terroristes et à leurs sympathisants un vivier mondial de recrues potentielles.

Les cyberforums à accès restreint offrent à ces recrues un lieu où s’informer sur les organisations terroristes, leur apporter leur soutien et participer directement à des actions en vue d’objectifs terro- ristes.

L’utilisation de verrous technologiques à l’entrée des plateformes de recrutement complique également la tâche du personnel des services de renseignement, de détection et de répression en matière de surveillance de l’activité terroriste.

Comme en exemple : Twitter

Twitter "était une plateforme de choix pour les djihadistes"

Ce positionnement a pris une tournure massive à la fin des années 2000 avec l'avènement des réseaux sociaux Facebook, Youtube, Twitter. Jusqu'ici, les djihadistes occupaient surtout des sites web et des forums. En 2014, le groupe Etat Islamique est à son apogée sur les réseaux. Des milliers de comptes diffusent en masse des contenus djihadistes sur de nombreuses plateformes. La prise de conscience a lieu avec l'attentat de Charlie Hebdo en janvier 2015.

https://www.google.fr/amp/s/www.franceculture.fr/amp/numerique/twitter-etait-une-plateforme-de-choix-pour-les-djihadistes

Solutions possibles

- ➔ **Clarifier et valider l’adoption des lois internationales déjà mises en place:** examiner systématiquement les politiques gouvernementales relatives aux

communications numériques et à la collecte de données à caractère personnel, et trouver les politiques qui portent atteinte à la vie privée sans justification valable;

- ➔ **Assurer que toutes les lois nationales sur la vie privée en ligne respectent les droits de l'Homme:** veiller à ce que les procédures et lois nationales relatives à la vie privée soient compatibles avec les obligations découlant de la Déclaration Universelle des Droits de l'Homme;
- ➔ **Examiner les responsabilités du secteur privé:** en suivant le cadre «Protégez, respectez et réparez» des Principes directeurs des Nations Unies, dans le contexte spécifique des technologies numériques de l'information et de la communication;
- ➔ **Encourager des normes internationales qui traitent la vie privée comme un droit:** voir le lien entre la vie privée, la liberté d'expression et d'autres droits de l'Homme dans le contexte numérique;
- ➔ **Travailler avec des experts de l'ONU:** sur la protection de la liberté d'expression, la liberté de réunion et d'association et les défenseurs des droits de l'homme, afin d'identifier des menaces spécifiques aux droits dans le contexte de la surveillance de masse, pour une approche plus globale de la protection de la vie privée
- ➔ **Stimuler les plateformes (ex: Facebook, Twitter, Instagram) à s'engager plus concrètement:** dans le suivi des signalements de leurs utilisateurs, dans l'éventuelle développement d'IA prévenant les hackeurs et piratage avant action, et dans leur coopération avec les polices de la cybercriminalité. Plus concrètement, dès qu'une remontée est faite par un utilisateur, celle-ci doit être analysée/ est une répondue dans les plus brefs délais. Et des engagements, entre le pays avec ses lois et la plateforme peuvent être établi (exemple : un IA détectant des scènes de violences, pour une suppression immédiate)

Pays et organisations impliqués

Algérie : ce pays ne dispose pas de lois sur les données privées , donc peut les utiliser librement car il n'est pas encadré.

Espagne: pays ou les données personnelles sont encadrés grâce au RGPD (Règlement général sur la protection des données) donc protégée, et ne dispose pas d'outils de transferts.

LA CNIL (Commission Nationale de l'Informatique et des Libertés)

Cette carte très détaillée vous permet de visualiser les différents niveaux de protection des données des pays dans le monde:
https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

DIGIT (European Commission Directorate General for Informatics)

Cette page détaille les responsabilités, de la commission à l'échelle européenne:
https://ec.europa.eu/info/departments/informatics/mission-statement-informatics_fr

Questions directrices

- Comment peut on définir des limites universelles à l'invasion de la vie privée sur internet?
- Quelles normes peut on mettre en place qui seront applicable pour tout gouvernement (avec l'un qui dépend énormément du contrôle en ligne et l'autre peut être pas du tout)
- Comment peut on renforcer les lois déjà existantes pour qu'ils ne se fassent pas ignorées?
- En sachant que les solutions doivent être "orienté vers le futur", comment peut on prendre en compte le développement constant et rapide de la technologie dans nos débats et nos résolutions? Que devons nous alors souligner ou clarifier pour qu'il n'y ait pas de lacunes?
- Comment peut on expliquer les risques des réseaux sociaux à la fois personnels mais aussi éthiques et politiques? Comment peut on les diminuer?

Bibliographie

https://www.hrw.org/news/2015/03/26/un-major-step-internet-privacy
https://www.un.org/fr/universal-declaration-human-rights/
http://gilc.org/privacy/survey/intro.html
https://www.francetvinfo.fr/internet/amazon/faut-il-se-mefier-des-assistants-vocaux-trois-exemples-d-espionnage-qui-incitent-a-la-prudence_2771149.html
https://www.jipitec.eu/issues/jipitec-8-4-2017/4641/
https://teachprivacy.com/privacy-data-security-violations-whats-harm/
Service public pro
https://www.service-public.fr/professionnels-entreprises/vosdroits/F24270

Le petit juriste
https://www.lepetitjuriste.fr/la-protection-des-donnees-personnelles-sur-internet/

https://www.contrepoints.org/2019/07/22/349557-internet-il-faut-proteger-votre-vie-privee

https://www.google.fr/amp/s/sawisms.blog/2016/10/09/dangers-reseaux-sociaux-vie-privee/amp/

https://www.cnil.fr/fr/proteger-sa-vie-privee-en-6-etapes

https://www.fnac.com/5-conseils-pour-proteger-sa-vie-privee-sur-le-net/cp38684/w-4

Europea.Eu
https://www.google.fr/amp/s/europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/indexamp_fr.htm

Peut-on vraiment se protéger ?
https://www.legavox.fr/blog/alexandre-chombeau/atteinte-privee-internet-peut-vraiment-21846.htm

Utilisation de l'Internet UNODC :
https://www.unodc.org/documents/congress/background-information/Terrorism/Use_of_the_Internet_for_Terrorist_Purposes_French.pdf