

Comité: Protection et Sécurité

Question: La protection des données sur internet

Membre de l'État-major : Kaan ARIBAL

Introduction :

Internet est devenu un outil essentiel dans nos vies et la révolution numérique est sans aucun doute le plus important bouleversement de ce début de XXI^e siècle. À quand remonte la dernière journée pendant laquelle nous ne nous sommes pas connectés une seule fois ? Internet a bouleversé notre façon de communiquer, d'accéder à l'information, de travailler, de nous divertir, de nous déplacer, de nous rencontrer, ou même de participer à la vie politique. On a vu apparaître des marchés dont l'infrastructure est totalement basée sur l'internet. On peut citer par exemple l'empire Facebook, qui a fait de Mark Zuckerberg, à 33 ans seulement, l'une des principales fortunes mondiales.

Au monde réel s'ajoute donc aujourd'hui le monde virtuel, de plus en plus important, de plus en plus puissant d'un point de vue économique. À notre vie réelle, s'ajoute désormais notre vie virtuelle, de plus en plus précieuse à nos yeux. Et si internet procure souvent un sentiment de liberté, de légèreté, les risques qu'il engendre sont pourtant nombreux et bien réels. Mais à quoi correspond ce monde virtuel ? Sur quoi internet est-il basé ? Sur des données, que l'on accumule, que l'on enregistre et transmet sans forcément y prendre garde, et qui peuvent ensuite être utilisées, vendues, achetées, volées... La question de la sécurité des données sur internet est essentielle dans le monde actuel. Et elle est d'autant plus importante qu'elle est encore relativement nouvelle. Bien sûr, les gouvernements ont établi des lois pour garantir la protection des données de leurs citoyens et des entreprises, il y a eu des conventions au sujet de la protection de données individuelles ainsi que des grandes données complexes ; mais il reste encore beaucoup à faire.

Définition des termes-clés

Données sur internet

Les données informatiques, c'est ce qui compose tout élément numérique. Les

données informatiques sont (pour l'instant) sous forme binaire (0 - 1). Autrement dit, une photographie ou un texte numériques, une application ou un site internet sont constituées de données. Ces données, nous les stockons sur nos ordinateurs, nos disques durs, mais aussi, de plus en plus, "sur internet", c'est-à-dire à distance, dans des centres de stockages (d'énormes disques durs, en quelque sorte) appelés *data centers*.

La cybersécurité

La cybersécurité est la sécurité sur internet. Il s'agit des techniques utilisées pour la protection de l'intégrité des réseaux, des programmes et des données contre les attaques, les dommages ou l'accès non autorisé.

L'anonymat sur le web

C'est la protection de l'identité de l'utilisateur sur internet (par exemple quand il utilise un moteur de recherche).

L'économie de l'internet

L'économie de l'Internet, ou économie numérique, fait référence à toutes les activités menées par des marchés dont l'infrastructure est basée sur l'Internet. Nous pouvons citer comme exemple AirBnb, devenue en très peu de temps la plus grande chaîne hôtelière du monde alors qu'elle ne possède aucun établissement hôtelier.

L'économie de l'Internet est constituée du commerce entre ces entreprises et l'utilisateur.

L'internet des objets

Considéré comme la troisième évolution de l'Internet, et aussi appelé « Web 3.0 », l'internet des objets consiste à connecter les objets de tous les jours à internet pour leur permettre d'envoyer et de recevoir des données sans avoir besoin d'une intervention humaine. Ainsi, les voitures sont de plus en plus connectées, et les maisons commencent à l'être. Par exemple, un réfrigérateur connecté va pouvoir détecter qu'il ne contient plus de lait et faire une commande de lait directement sur internet, sans que l'homme n'ait besoin d'intervenir.

L'art antérieur

L'art antérieur correspond à l'ensemble des éléments déjà brevetés. Si on essaie d'obtenir un brevet pour une invention, il faut que cette invention soit réellement nouvelle. Pour le vérifier, on la compare avec l'art antérieur.

Aperçu général

Big Data

Le « Big Data », parfois appelé mégadonnées ou encore données massives, correspond aux gigantesques quantités de données que produisent nos appareils connectés : nombre de pas que nous faisons chaque jour, nombre d'heures de sommeil, recherches faites sur internet, temps passé sur chacune des pages consultées, itinéraire effectué chaque jour, achats en ligne, type d'informations lues sur les réseaux sociaux, centres d'intérêts, etc. L'analyse de ces données est une mine d'or pour les entreprises, car elle permet de connaître bien mieux ses clients, et donc d'adapter ses produits, d'affiner son offre, de cibler ses publicités... Mais elle sert également aux partis politiques, par exemple, afin de mieux connaître ses électeurs potentiels et donc d'adapter sa stratégie en fonction des informations reçues.

La complexité de ces données implique qu'elles ne peuvent pas être traitées par un système de gestion de bases de données classique (SGBD). Une autre technologie est nécessaire, appelée "Big Data Analytics".

Cependant, l'utilisation du Big Data crée certains problèmes. Premièrement des problèmes de sécurité apparaissent. Etant donné que le Big data correspond à une énorme quantité de données, les réseaux de Big Data sont une cible privilégiée des cyberattaques. Or comme l'analyse du Big Data est relativement nouvelle, ces problèmes de sécurité ne sont pas bien résolus. Par exemple, aux Etats-Unis, le réseau de Big Data scolaire « Inbloom » s'est écroulé. La protection des données n'était pas suffisante et l'existence du réseau causait l'inquiétude des parents d'élèves.

Les technologies actuelles, l'internet des objets ainsi que les innovations possèdent des avantages ainsi que des inconvénients, notamment des problèmes de sécurité. L'essentiel c'est de bien gérer ces problèmes sans limiter les avantages potentiels.

Big Data et propriété intellectuelle

Quels liens y a-t-il entre le Big data, le “Big data analytics”, les quantités des données sur internet et la propriété intellectuelle ? Pour qu’un brevet soit accordé, il faut avant tout que l’invention soit réellement nouvelle, originale. En d’autres termes, si on trouve un “art antérieur”, donc un ou des brevets pour une invention similaire à ce qui est proposé, alors le brevet ne sera pas accordé. Mais comment rechercher l’art antérieur ? Une recherche sur un moteur de recherches peut donner à peu près 100.000 résultats, qu’il est impossible de consulter en intégralité. On estime que la quantité de données sur internet double tous les 18 mois.

Le “Big Data Analytics” peut être utilisé pour analyser une grande quantité de données, comme 100.000 documents. Les gouvernements n’ont pas encore l’habitude d’utiliser cette méthodologie, alors il y a des brevets qui sont accordés mais qui normalement ne devraient pas l’être car il existe un art antérieur¹. Le Big data analytics permettra une vérification plus précise, et donc plus juste.

L’économie de l’internet

Internet a sans doute augmenté notre capacité à créer, communiquer, coordonner et innover. Par exemple, le gouvernement électronique (qui implique l’utilisation de l’internet et des technologies de l’information par le gouvernement pour améliorer la qualité des services publics, renforcer la participation des citoyens par l’accès à l’information) est devenu un outil essentiel pour soutenir les fonctions gouvernementales et l’interaction avec les citoyens et les entreprises. Ainsi les gouvernements, les producteurs et les consommateurs sont dépendants de l’Internet. Ces interactions entre eux créent l’économie de l’Internet.

L’économie numérique est constituée de toutes les activités de production et de consommation qui ont lieu sur internet. Et elles sont de plus en plus nombreuses, car internet rend l’activité économique plus rapide et moins coûteuse. En effet, elle réduit notamment le coût des transactions. Dans un [rapport](https://dataflog.com/read/innovation-and-big-data/525) l’Organisation de coopération et de

¹ <https://dataflog.com/read/innovation-and-big-data/525>

développement économiques (OCDE) relève que le secteur de l'Internet est l'un des seuls secteurs en nette croissance, malgré la crise économique.

Cette nouvelle économie a beaucoup d'aspects positifs mais aussi des dangers. Bien qu'internet ait une nature libre, il lui faut des régulations pour protéger l'internaute.

L'économie de l'Internet et la propriété intellectuelle

Rifat Atun, Ian Harvey et Joff Wild ont constaté que les brevets qui protègent la propriété intellectuelle contribuent à la croissance économique² dans la mesure où le principe des brevets pousse à l'innovation. Pour Rifat Atun, Ian Harvey et Joff Wild l'innovation est le facteur le plus important pour la croissance économique à long terme. En conséquence la protection de toute forme de propriété intellectuelle a une corrélation avec l'originalité et l'innovation, ce qui contribue au développement de l'économie, qu'elle soit "traditionnelle" ou numérique.

La protection des données

La protection des données, également appelée "confidentialité des données" ou "confidentialité des informations", se fait à différents niveaux. Il existe une protection des données au niveau personnel, il y a celle des entreprises ou des entités publiques, et celle des données "sensibles" qui nécessitent une protection renforcée. Il s'agit à la fois de l'intégrité des données, de la protection contre la corruption ou les cyberattaques et du contrôle de l'accessibilité des données (qui ne doivent être accessibles qu'aux personnes autorisées).

L'enjeu est de protéger de manière efficace les données confidentielles, sans pour autant mettre un frein à l'utilisation d'internet et à son potentiel, à la fois du côté de l'internaute, et du côté des entreprises, qui devraient par exemple pouvoir utiliser le Big data à des fins professionnelles.

La protection des données est importante pour l'économie d'un pays. Elle est directement liée au commerce des services. Une protection insuffisante peut créer des effets négatifs sur le marché en réduisant la confiance des consommateurs, par exemple dans le cas d'une banque ou d'un service de messagerie électronique qui se serait fait pirater (nous avons tous en mémoire le piratage massif de comptes Yahoo, qui a sérieusement réduit la confiance

² Lien vers [l'article](#).

des utilisateurs envers cette entreprise). En même temps une protection trop rigoureuse peut être un handicap aux entreprises et avoir des effets négatifs sur l'économie.

La place des gouvernements dans la protection des données

Les gouvernements doivent-ils s'impliquer dans la protection des données ? S'il s'agit des données confidentielles récoltées par l'État (santé, impôts, défense nationale...), cela va de soi. Mais qu'en est-il des données personnelles des citoyens, ou des données des entreprises ? S'il appartient à chacun, citoyen ou entreprise, d'être attentif à la confidentialité de ses propres données, en réglant correctement ses paramètres de confidentialité, en choisissant des codes secrets appropriés, en prenant garde à ne pas télécharger une pièce jointe douteuse, etc (de la même manière qu'on ferme la porte de sa maison ou qu'on cache son code de carte bancaire quand on retire de l'argent), l'État doit-il intervenir, notamment en légiférant ? Il semble difficile de ne pas le penser : l'État a entre autres comme devoir d'assurer la sécurité de ses citoyens.

Au 21^{ème} siècle, le système économique mondial est dominé par le néolibéralisme, basé sur le marché libre. Mais même s'il est libre, il lui faut des régulations. C'est aussi le cas de l'économie de l'Internet. Sans l'intervention du gouvernement il est impossible d'empêcher que des problèmes de sécurité apparaissent. C'est donc le devoir du gouvernement de prendre des mesures afin de garantir la sécurité de toutes les parties incluses. Néanmoins, le gouvernement doit collaborer avec le secteur privé pour que les lois adoptées ne soient pas trop handicapantes pour les entreprises.

Cette question d'une forme de contrôle d'internet par les gouvernements est liée à celles, plus générales, de la censure, de la liberté et du respect de la vie privée. Faut-il censurer des sites dangereux pour la sécurité des citoyens, et notamment la sécurité de leurs données ? Oui, certainement, de la même manière qu'un individu qui vole des données doit être condamné et mis hors d'état de nuire. Faut-il au contraire, dans certains cas, que l'État puisse accéder aux données personnelles d'un citoyen (de la même manière qu'il ferait une perquisition dans son appartement) pour protéger d'autres citoyens ?

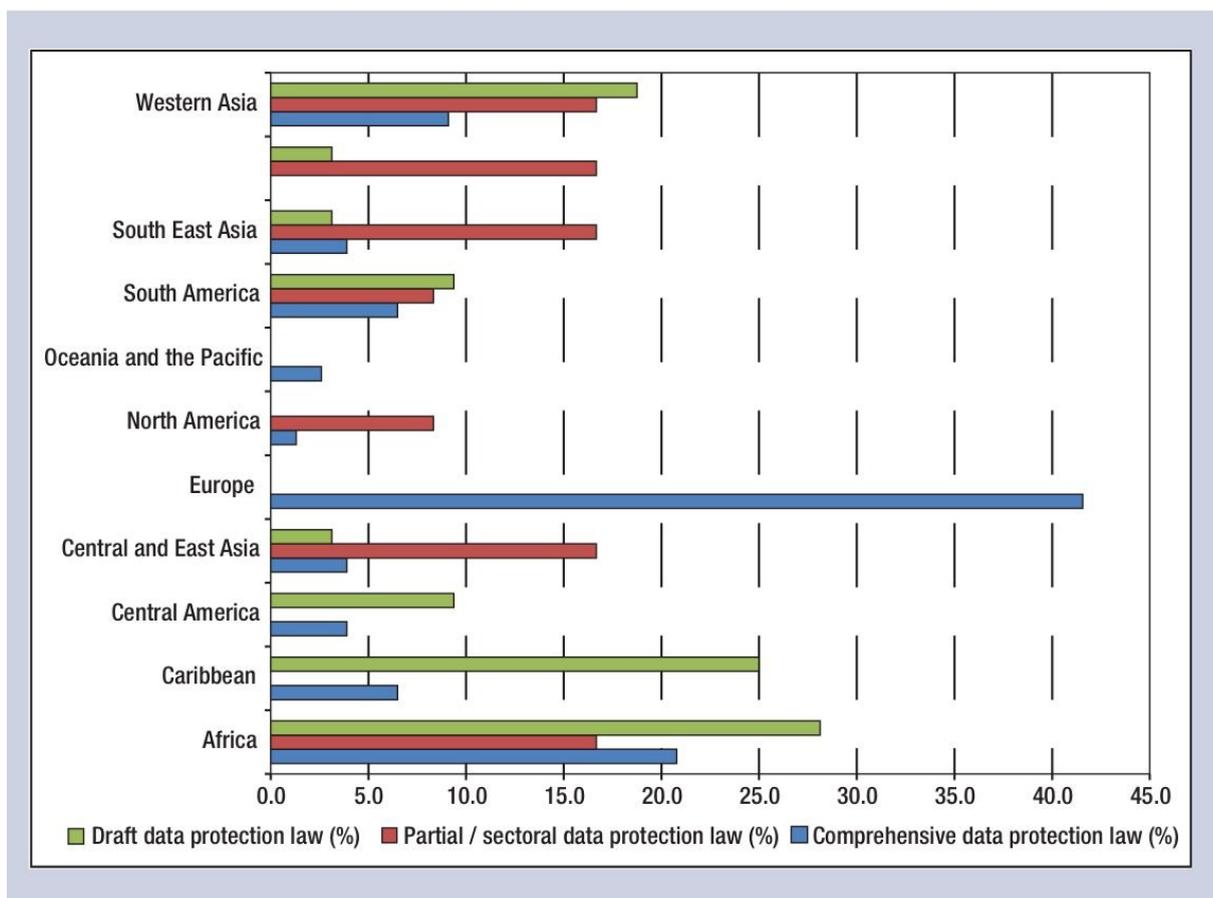
Cette question de la surveillance d'internet s'inscrit donc dans la question générale de la protection des citoyens : pour pouvoir protéger, il faut pouvoir surveiller et contrôler. Néanmoins cette surveillance doit être elle-même contrôlée et limitée, car sinon cela nuit à la liberté et à la vie privée des citoyens. Cette question est pleinement d'actualité, avec les "états

d’urgence” adoptés en ce moment par un certain nombre de pays et qui modifient le rapport habituel entre surveillance de l’État et vie privée des citoyens.

Mais surtout, cela pose la question du statut du Big Data : ces immenses quantités de données que nous produisons nous appartiennent-elles ? Dans quelle mesure peut-on laisser des entreprises stocker ces informations sur nous ? Dans quelle mesure les entreprises peuvent-elles revendre ces informations qu’elles ont sur nous ? Une application peut-elle obliger ses utilisateurs à lui céder les données qu’ils produisent (par exemple, une application de cartographie peut-elle obliger ses utilisateurs à accepter qu’elle récolte des informations sur tous leurs déplacements, dans le but de les revendre à des entreprises) ?

Inversement, si cela est indiqué dans des conditions d’utilisation et que l’utilisateur accepte ces conditions, l’État doit-il ou peut-il intervenir ?

Figure 4. Global percentage of comprehensive, partial/sectoral and draft data protection laws in each region



Source: UNCTAD

Dans le graphe au-dessus on observe la situation des états du monde face aux problèmes de protection des données. Il y a trois types de loi qui concerne la protection des données. Le premier appelé “Draft data protection law” sur le graphe est simplement en projet de loi qui vise à devenir un loi. La deuxième est appelé “Partial Sectoral data protection law” sur le graphe. Cette dernière fait référence aux lois qui concerne un domaine spécifique par exemple les lois qui se concentre sur le secteur privée. La troisième qui est appelé “comprehensive data protection law” sur le graphe est l’ensemble des lois destinées de faire face aux problèmes concernant la protection des données d’une manière impartial et générale.

Pays et organisations concernés

La France

La France est un exemple de pays où les lois sur la protection des données sont fortes et bien établies. La France a aussi des lois qui concernent le flux des données avec d’autres pays. Il y a trois cas possibles :

- le transfert avec des pays membres de l’Union européenne ne nécessite pas d’autorisation ;
- le transfert de données entre la France et les pays qui, selon l’Union européenne, ont établi une protection efficace³, nécessite juste une notification ;
- quant au transfert de données avec d’autres pays, il n’est pas autorisé.

La Commission nationale de l’informatique et des libertés (CNIL) est une autorité administrative qui joue un grand rôle, en France, dans le domaine de la protection des données. Elle a pour mission de garantir que la loi sur la protection des données est bien appliquée dans tous les domaines de la vie. Son existence a été établie par la loi française ([loi n° 78-17](#)) du 6 Janvier 1987.

Le Brésil

Le Brésil peut être montré comme un bon exemple de pays qui essaie de mettre des lois en place. Ainsi, il a développé un “projet de loi” (qui n’a pas encore été adopté) sur la

³ Voir ci-dessous, la partie sur l’Union européenne

protection des données en janvier 2015. Ce projet est basé sur la “[directive sur la protection des données](#)” adoptée par l’Union européenne.

Le Royaume-Uni

Le Royaume-Uni est aussi un exemple de pays où la protection des données est bien garantie. Le “[Data protection act](#)” établi en 1998 est une loi qui définit les droits d’un propriétaire de données, ainsi que les principes des protections des données. Elle met l’accent aussi sur le consentement. En conclusion il vise à garantir la protection des données de toute forme tout en respectant l’intimité des citoyens.

Union européenne

En 1995, l’Union européenne a adopté une directive appelée la “[directive sur la protection des données](#)” qui montre l’importance de la collaboration de tous les États membres sur la problématique de la protection des données. Notamment, cette directive empêche les membres de l’Union européenne de transférer des données aux pays pour lesquels la protection est jugée insuffisante. Bien entendu, la liste des pays considérés comme sûrs du point de vue de la protection des données est régulièrement mise à jour. Ainsi, elle a accueilli le Canada en 2002, l’Argentine en 2003, la Suisse et l’île de Man en 2004, Jersey en 2008, Andorre et les Îles Féroé en 2010, Israël en 2011, l’Uruguay en 2012 et la Nouvelle-Zélande en 2013. De manière plus générale, cette directive est toujours amendée et améliorée afin qu’elle soit adaptée au monde actuel.

Coopération Économique Asie-Pacifique (APEC)

L’APEC, qui est composée de 21 membres qui au total représentent 41% de la population mondiale, a pris quelques initiatives sur la protection des données ([UNCTAD/34](#)). L’APEC a notamment créé des règles. Le but de ces dernières est d’établir des principes qui s’appliquent à tous les États membres pour rendre possible le transfert de données sur internet entre les pays en garantissant leur protection. Etant donné que le flux libre des données est très important pour la durabilité économique dans notre monde libéral, les règles de l’APEC favorisent et facilitent le commerce.

Le Conseil Européen

La Convention sur la protection des données du Conseil de l'Europe⁴ (aussi appelée la "convention 108") est la convention pendant laquelle ont été prises les premières initiatives mondiales dans le domaine de la protection des données informatiques. Cette convention, essentielle dans la protection de la vie privée, met l'accent sur le flux transfrontalier et elle déclare que les données personnelles qui révèlent les idées politiques, religieuses ou les données qui sont liées à la vie sexuelle ou encore celles qui révèlent les problèmes de santé ne peuvent pas être traitées d'une manière automatisée. Les avantages de cette convention sont les suivants : elle vise à adopter des principes communs pour garantir la sécurité des données, c'est une collaboration de tous les pays signataires ; elle vise à trouver une solution globale pour faciliter le flux des données en garantissant la sécurité ; et enfin, même si cette convention a été établie par le Conseil européen, elle concerne également des pays qui ne sont pas des pays européens.

L'Organisation de Coopération et de Développement Économiques (OCDE)

[Les lignes directrices de l'OCDE⁵](#) sur la protection de la vie privée et sur la protection des données ont été publiées en 1980 mais il y a eu des amendements et les lignes ont été révisées en 2013. Ces lignes ont eu un impact mondial. En effet, ces lignes directrices constituent les principes de la plupart des lois nationales sur la protection de la vie privée. Ces lignes directrices aident les gouvernements et les entreprises à protéger la vie privée et les données personnelles, tout en évitant des restrictions inutiles et nuisibles aux flux transfrontaliers de données.

Les Nations Unies

Pendant les années 2013-2015, les Nations Unies ont renforcé leur rôle dans la protection des données et la vie privée en prenant deux mesures fondamentales. La première c'était la publication d'une [résolution](#) sur la protection des données. Cette résolution met l'accent sur l'importance de l'intimité de la vie privée et sur les problèmes éthiques qui apparaissent avec la surveillance et l'interception de la communication. La deuxième mesure était l'embauche d'un rapporteur expert dans le domaine de la protection des données sur l'Internet, M. Joseph Cantanaci. Celui-ci a écrit un rapport ([A/HRC/31/64](#)) sur l'intégrité de

⁴ <http://www.coe.int/fr/web/data-protection/home>

⁵

<http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontiersdedonneesdecaracterepersonnel.htm>

la vie privée et sur la protection des données personnelles. Pour les années à venir, les Nations Unies visent à soutenir les pays en développement en établissant des programmes de développement des compétences.

Solutions possibles

Adoption de lois

Cette solution, comme mentionné dans le rapport tout entier, est la solution la plus efficace possible. Il existe dans le monde certains pays qui n'ont aucune loi sur la protection des données. Dans ces pays, les droits de propriété intellectuelle pour les données sur internet ne sont pas respectés et il existe un grave problème de « vol de données ».

Les Nations Unies jouent un rôle important en aidant les pays en développement dans la mise en place des lois sur la protection des données, ce qui est essentiel non seulement pour établir la confiance sur les activités numériques mais aussi pour la participation à l'économie de l'Internet. La mise en place des lois pertinentes favorise le développement des nations émergentes.

Renforcement de la police du web

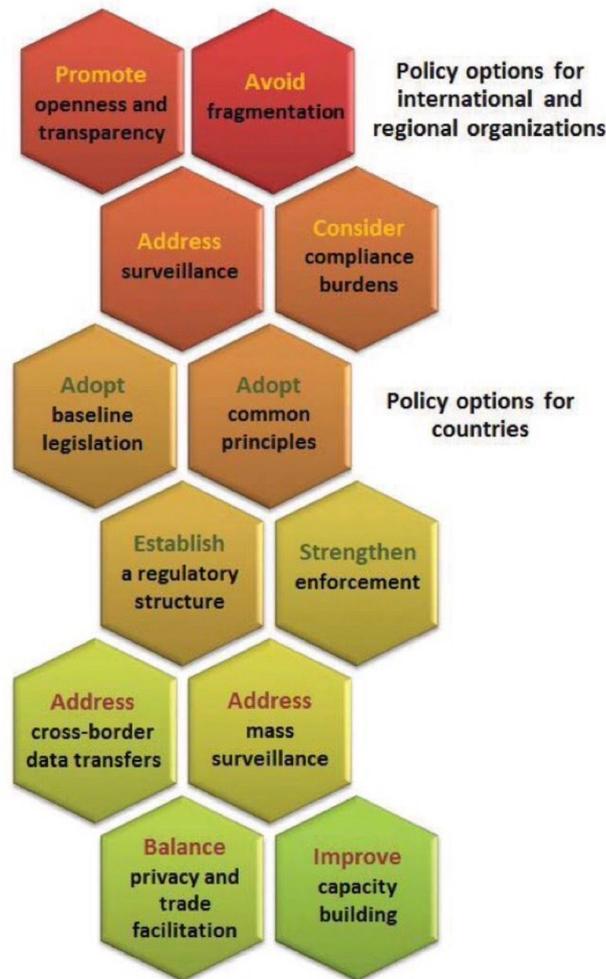
Une fois que les lois sont adoptées, il faut les faire appliquer. Pour cela, il faudrait renforcer la police du web pour pouvoir mieux combattre ce fléau.

Adoption de principes

Les principes ne sont pas exclusivement basés sur la loi mais ils ont un but commun avec la loi. Ils diffèrent cependant des lois sur un point important : les principes sont universels et ils ne sont pas obligatoires. Les entités publiques et privées peuvent adopter des principes qui soutiennent la protection des données. On peut mentionner par exemple la

[résolution 45/95](#) de l'Assemblée Générale des Nations-Unies, qui a été adoptée le 15 décembre 1989.

Figure 6: Key Policy Options



Source : UNCTAD

Comme on le voit sur cette infographie, il existe certaines mesures à prendre pour garantir la protection des données. Les deux qui se trouvent au centre, ce sont les solutions qui se trouvent à la base de toutes les autres. Il s'agit d'établir des lois et d'établir des principes. Les solutions en rouge, ce sont des solutions destinées aux organisations internationales. Quant aux solutions qui sont en vert, ce sont plutôt des solutions générales qui mettent l'accent sur une problématique globale à laquelle il faut réfléchir. En conclusion,

bien que trois solutions aient été développées dans le rapport, il en existe d'autres proposées sur cette infographie.

Rapport de cas

Au mois de juin 2013, Maximilian Schrems, un avocat bien connu, a fait une réclamation contre Facebook pour empêcher Facebook de transférer ses données collectées en Europe sur le réseau aux Etats-Unis. Il a mis en avant le fait que le « EU-US Safe Harbor Framework » n'assurait pas un degré de sécurité suffisant pour les données privées des citoyens de l'Union Européenne.

Sa réclamation a été rejetée étant donné que Facebook était un membre de « EU-US Safe Harbor Framework ». Cette décision a été référée au tribunal Irlandais qui à son tour l'a transmise à la cour de justice de l'Union Européenne.

La cour de justice de l'Union Européenne est parvenue à l'idée que la réclamation de Maximilian Schrems devait être à nouveau étudiée et après examen du cas elle a reconnu que les mesures que prenait le « EU US Safe Harbor » n'assuraient effectivement pas une protection suffisante. Cette décision est particulièrement importante car elle a un impact sur le commerce entre l'UE et les Etats-Unis.

En outre, la Cour de justice a estimé que la législation qui permet aux autorités d'accéder à des informations personnelles, pour des raisons liées à la sécurité nationale, sans l'autorisation de l'individu, étaient en contradiction avec les droits fondamentaux des citoyens de l'UE.

Ce rapport de cas souligne notamment la nécessité d'avoir des lois cohérentes au niveau international, puisque l'économie numérique se fait au niveau mondial.

Deuxième rapport de cas

Benesse est une grande entreprise dans le domaine de l'éducation. Au mois de juin 2014, l'entreprise a été piratée et une grande quantité de données appartenant à des élèves et leurs familles ont été volées. On a constaté qu'un ingénieur avait volé les données et les avait vendues à une entreprise rivale. Après cet incident Benesse a été gravement endettée.

Bibliographie

"Data Protection Regulations and International Data Flows: Implications for Trade and Development" , 2016.

http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

"2013 OECD Privacy Guidelines,." Web. 2013.

<http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>

"Resolution Adopted by the General Assembly on 18 December 2013" 18 Decembre 2013.

http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

"Economie de l'Internet : une économie d'interactions sociales" Avril 2007

<https://perso.univ-rennes1.fr/thierry.penard/biblio/Interactionsociale.pdf>

"L'Internet, un moteur de croissance pour l'économie mondiale,04/10/2012

<http://www.la-croix.com/Actualite/Economie-Entreprises/Economie/L-Internet-un-moteur-de-croissance-pour-l-economie-mondiale- NG -2012-10-04-860833>

"L'économie de l'Internet" Avril 1997

<http://www.lajauneetlarouge.com/article/leconomie-de-linternet#.WcJ AdFRWhA>

"Le futur de l'économie Internet, Réunion ministérielle de l'OCDE, Séoul, Corée du Sud" les 17 et 18 juin 2008

<https://www.oecd.org/fr/futurinternet/39162655.pdf>

"Les 7 principes clés de la protection des données personnelles"Page publiée le 19 octobre 2011 mise à jour le 18 janvier 2012

<http://www.cil.cnrs.fr/CIL/spip.php?article1390>

"Analyse d'impact relative à la protection des données"

<https://www.gdpr-expert.eu/article.html?id=35#textesofficiels>

"Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère

personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)” 27 avril 2016

<http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679>

“Report on a comprehensive approach on personal data protection in the European Union”
22 Juin 2011

[http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2011-0244
&language=EN](http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2011-0244&language=EN)

“Enquiries Into Intellectual Property’s Economic Impact” 2015

<http://www.oecd.org/sti/ieconomy/KBC2-IP.Final.pdf>

“Privacy and data protection principles”

<http://www.unglobalpulse.org/privacy-and-data-protection-principles>

“Aspects de l'économie de l'Internet, Octobre 1999”

<http://barthes.ens.fr/atelier/articles/serval99.html>

“Innovation brevets et la croissance économique, Juin 2007”

https://www.researchgate.net/profile/Rifat_Atun/publication/23751118_INNOVATION_PATENTS_AND_ECONOMIC_GROWTH/links/09e4150b1ff5dbf7de000000/INNOVATION-PATENTS-AND-ECONOMIC-GROWTH.pdf

“Data Gueule, *Données, données, donnez-moi*, Date gueule n°15, *Youtube*, 15 novembre 2014”

<https://www.youtube.com/watch?v=5otaBKsz7k4>

“Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 1981”

<https://rm.coe.int/1680078b37>