COMITÉ : Cybersécurité mondiale
PROBLÉMATIQUE : Comment les institutions internationales peuvent-elles encadrer l'utilisation des données personnelles afin de prévenir leur exploitation commerciale, la surveillance étatique et les risques liés aux cyberattaques ?
PRÉSIDENTS : Anouchka WEISROCK, Indri SELIMI, Hicham FOFANA

PRÉSENTATION DE LA PRÉSIDENCE



Bonjour à toutes et à tous !

Je m'appelle Anouchka WEISROCK, élève à Ferney-Voltaire en section internationale anglaise. Je parle trois langues : le français, le hongrois et l'anglais. Je suis passionnée de sport : je pratique le golf à un niveau compétitif et j'apprécie également le tennis ainsi que le volley. En parallèle, je joue du piano au conservatoire et j'aime beaucoup la peinture à l'huile, une activité qui me permet d'exprimer ma créativité. L'année dernière, j'ai intégré le MUN en tant qu'admin de résolution. Cette expérience m'a permis de découvrir en profondeur l'organisation et le fonctionnement du MUN, ainsi que le rôle de président, qui m'a particulièrement intéressée. Durant la conférence FerMUN 2027, notre comité s'intéressera à la protection des données personnelles, une question devenue essentielle à l'ère du numérique. Ces informations occupent aujourd'hui une place centrale dans nos communications et nos échanges, mais elles attirent de plus en plus l'attention d'acteurs capables d'en détourner l'usage. Ainsi, nous chercherons des solutions concrètes pour sécuriser ces données et protéger la confidentialité des informations.

Je vous attends avec impatience à FerMUN 2027 !

MOTS-CLÉS

Institutions internationales[1] : Une institution internationale est une organisation créée par des Etats, dotée d'un traité ou d'une constitution, destinée à faciliter la coopération entre pays sur des questions communes. Elles poursuivent des buts précis et partagés, comme la coopération économique (FMI, Banque mondiale), la sécurité (OTAN), la santé publique (OMS) ou les droits humains (ONU).

Données personnelles[2] : une donnée personnelle est une information propre à une personne physique, se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, telle que son prénom, son nom, son adresse mail, l'adresse de son domicile etc…
Ces données peuvent être:
Directe : lorsqu'elles sont directement recueillies auprès de la personne concernée (Données collectées directement : lorsqu'elles sont recueillies auprès de la personne concernée, par exemple au moyen d'un formulaire).
Indirecte : lorsqu'elles ne sont pas fournies par la personne concernée mais collectées automatiquement. (Données collectées indirectement ou automatiquement : lorsqu'elles sont obtenues autrement qu'auprès de la personne concernée, par exemple par l'intermédiaire de tiers ou de certains traceurs. Attention : collecte directe/indirecte et identification directe/indirecte sont deux notions différentes).

Les entreprises sont soumises à diverses obligations ayant vocation à protéger la collecte et le traitement de ces données.

Exploitation commerciale[3] : constitue une activité économique toute forme d'exploitation d'un bien corporel ou incorporel en vue d'en retirer des recettes ayant un caractère de permanence. De plus, des entreprises utilisent les données personnelles des individus pour en tirer un profit et un avantage économique. En effet, grâce à la collecte massive de données personnelles, elles peuvent cibler précisément leurs campagnes publicitaires, ajuster les prix, optimiser leurs stratégies marketing et ainsi développer leurs ventes.

---

[1] Les institutions internationales | Secondaire | Alloprof.
[2] Donnée personnelle ou donnée à caractère personnel définition - Definition-juridique.fr

[3] https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000005634379/LEGISCTA000006179001/?utm

Surveillances étatiques[4] Les technologies de surveillance ont considérablement évolué ces dernières années, offrant aux États des capacités sans précédent. La vidéosurveillance, l'interception des communications, la collecte de métadonnées et l'utilisation de logiciels espions sont autant d'outils à la disposition des services de renseignement. Ces techniques soulèvent des questions éthiques et juridiques importantes, notamment en ce qui concerne le respect de la vie privée et la présomption d'innocence.
Par exemple, L'affaire Edward Snowden[5] en 2013 révèle une surveillance de masse menée par le NSA (National Security Agency) aux Etats-Unis. Les révélations d'Edward Snowden ont mis en évidence l'ampleur des capacités de surveillance électronique de la NSA, notamment la collecte massive de données et de métadonnées

Cyberattaques[6] : une cyberattaque est une attaque menée via le cyberespace dans le but de perturber, désactiver, détruire et de contrôler de manière malveillante un environnement informatique, ou de compromettre l'intégrité des données ou de voler des informations. Certaines cyberattaques ont pour objectif de voler des données afin de les exploiter ou de les revendre ; d'autres poursuivent des objectifs d'espionnage, de sabotage, d'extorsion ou de déstabilisation

Big data[7] : Cela consiste à collecter et analyser des données provenant d'un très grand nombre de personnes, d'appareils ou de sources. Ces données peuvent être utilisées à différentes fins, comme améliorer les opérations, proposer un meilleur service, faciliter la prise de décision, mieux comprendre certains phénomènes ou encore personnaliser des services. Le Big Data peut ainsi être mobilisé dans de nombreux domaines**.**

Les data brokers[8] **sont** des intermédiaires clés dans la collecte des données, ce sont les acteurs qui achètent, structurent, organisent et revendent les données ou des informations/profils issus de données provenant de différentes sources.

GAFAM[9] **:** est un acronyme désignant cinq grandes entreprises technologiques américaines. Ces lettres font référence aux cinq plus grosses entreprises du secteur: Google, Apple, Meta (anciennement Facebook), Amazon, et Microsoft.

---

[4] La surveillance étatique face aux libertés individuelles : un équilibre fragile | Actus Juridiques
[5] Edward Snowden, un lanceur d'alerte déterminé | INA
[6] csrc.nist.gov/glossary/term/cyber_attack
[7] Big Data : définition, technologies, utilisations, formations
[8] Courtiers en Données : Qui Vend Vos Infos Personnelles ?
[9] GAFAM — Wikipédia

APERÇU GLOBAL

La population actuelle dépend de plus en plus de la digitalisation via les plateformes numériques, les réseaux sociaux et les services en ligne avec 74% de la population mondiale connecté à internet depuis 2025 d'après l'UIT (Utilisateurs d Internet (% de la population) | Data).
Ainsi, chaque interaction en ligne, qu'il s'agisse d'un achat, d'une recherche ou d'un déplacement, peut générer de potentielles informations collectées ou analysées. Par ailleurs, le développement de l'IA pourrait contribuer à encore plus facilement accéder aux données personnelles d'un individu. De plus, ces données personnelles circulent en permanence, d'un pays à un autre, d'un serveur à un autre et même d'une entreprise à une autre. Par conséquent, cet accès facile aux données personnelles peut entraîner des usages abusifs, que ce soit par des entreprises pour gagner de l'argent, par les Etats pour assurer la sécurité et prévenir la criminalité, ou encore par les cybercriminels pour un éventuel vol ou pour une action malveillante.

I. Comprendre le flux des données et les acteurs

A. Les étapes de la circulation des données personnelles

Lorsqu'un individu navigue sur un site web, une application ou un service bancaire numérique, il laisse deux types de données personnelles.
D'une part, il fournit volontairement certaines informations telles que son adresse e-mail, son numéro de téléphone, ses coordonnées de paiement, qu'il saisit lui-même dans des formulaires ou des espaces dédiés.
D'autre part, au cours de sa navigation d'autres données sont collectées automatiquement, sans action directe de l'utilisateur. Il peut s'agir de données de géolocalisation, du type de l'appareil utilisé etc…

L'ensemble de ces informations est saisi par l'utilisateur ou collecté automatiquement. Puis, ces informations sont regroupées et enregistrées dans un système numérique.

Certaines données collectées par les applications ou les sites peuvent être transmises à des entreprises partenaires, selon les services utilisés, les finalités du traitement et le cadre juridique applicable. Ces partenaires peuvent être des plateformes publicitaires, permettant aux entreprises de mieux cibler leurs campagnes publicitaires ou des plateformes de services d'analyse ainsi que des data brokers.

Ensuite, certaines de ces données peuvent être agrégées par de grandes plateformes ou des data brokers (des courtiers de données). Une fois regroupées, elles sont croisées et organisées pour créer des profils plus détaillés d'individus ou de catégories d'individus.

Enfin,certains data brokers commercialisent, concèdent sous licence ou mettent à disposition des données, segments ou profils constitués à partir de différentes sources. Ils les transmettent à plusieurs acteurs, comme des entreprises (par exemple des banques) ou des marketeurs, pour des usages précis. Les plateformes, elles, peuvent exploiter les données dans leurs propres écosystèmes publicitaires sans nécessairement vendre directement les données personnelles elles-mêmes, elles les exploitent pour personnaliser leurs services ou diffuser de la publicité personnalisée. En cas de piratage, les données sont volées par des cybercriminels. Ce n'est pas un partage normal mais un accès illégal.

B. Les acteurs principaux

Les **data brokers**[10] sont des acteurs importants de l'écosystème de collecte et de commercialisation des données, ce sont les acteurs qui achètent, structurent, organisent et revendent les données. D'après Lunyb[11], le marché mondial des data brokers est estimé à plus de 250 milliards d'euros en 2026. Ce chiffre pourrait évoluer au cours des années en fonction des conditions économiques. Leur rôle est de créer des profils plus ou moins détaillés, et ensuite de les revendre à des marketeurs, des banques, des recruteurs, des acteurs politiques etc…

De plus, les **plateformes numériques** telles que Google (Android, Youtube, Maps , Gmail), Meta (Facebook, Instagram WhatsApp), tiktok (Bytedance) sont parmi les acteurs majeurs de la collecte et du traitement de données à grande échelle. Contrairement aux data brokers, elles ne les vendent pas directement mais génèrent des profits publicitaires grâce à leur exploitation.

Les **entreprises classiques**[12] (banques assurance, télécoms, magasins) sont des acteurs qui collectent leurs propres données et certaines d'entre elles utilisent les services des data brokers. Ainsi, les banques utilisent des données pour évaluer notamment la solvabilité d'un client et également pour faire de la publicité personnalisée.

---

[10] Courtiers en Données : Qui Vend Vos Infos Personnelles ?
[11] Courtiers en Données : Qui Vend Vos Infos Personnelles en 2026 ?
[12] Demandes de crédit : comprendre l'utilisation de vos données et vos droits | CNIL

Les **Etats et institutions publiques**[13] ont leurs propres sources de données mais peuvent aussi acheter des données de géolocalisation ou de navigation auprès des data brokers. Ils utilisent ces données pour le renseignement, la sécurité et les enquêtes.

Les **cybercriminels** ne sont pas des acteurs légitimes car ils utilisent les données pour commettre des fraudes, des extorsions et des usurpations d'identité, afin d'en tirer un profit. Les données sont soit volées par piratage, ransomware ou phishing. Soit elles font l'objet de fuites, notamment à la suite d'erreurs humaines ou de failles de sécurité, ou bien elles sont revendues sur des marchés clandestins.

II. Les différents risques induits par la multiplication des données

Premièrement, lorsqu'un service numérique collecte les données personnelles d'un individu, cela peut entraîner une perte de maîtrise ou, en cas de traitement abusif ou de fuite, une atteinte à la confidentialité de certaines données telles que son identité, ses achats, sa navigation sur internet, sa localisation…
Souvent, la population n'est pas au courant et surtout n'a pas accepté ce transfert de données. Ce qui pourrait favoriser des pratiques abusives, notamment à travers les trois types de menaces présentés ci-dessous.

A. Risque commercial

Les données collectées ou traitées à des fins commerciales peuvent être utilisées pour influencer le comportement d'une personne, en orientant ses choix ou ses décisions sans qu'elle en ait conscience. Ces personnes peuvent être davantage exposées à des stratégies de ciblage commercial susceptibles d'influencer leurs comportements. Par exemple, un individu qui cherche des informations sur un problème de santé peut recevoir des publicités pour des traitements excessivement chers, ou une personne en difficulté financière peut être submergée d'offres de crédits risqués ce qui pourrait potentiellement conduire à une situation de surendettement.
De plus, de nombreuses entreprises du secteur financier, de l'assurance ou du recrutement utilisent des données pour évaluer le profil d'un individu et sa solvabilité. Par exemple, une banque peut refuser un crédit ou proposer un taux d'intérêt plus élevé en fonction de critères de risque et de solvabilité, dans le respect de la réglementation applicable.

[13] Le FBI achète les données de géolocalisation des citoyens US : et en France ?
Data Brokers : un marché opaque au cœur des menaces informationnelles - Semkel

B. Risque Etatique[14]

Les données peuvent être également utilisées par des gouvernements et leurs services de renseignement ce qui peut accroître les capacités de surveillance sur la vie privée d'un individu et pourrait menacer sa liberté individuelle. Dans certains pays non-démocratique, (tels que la Chine, la Russie, la Corée du Nord ou bien l'Iran), ces données servent à surveiller des activistes, des journalistes ou des opposants politiques ce qui peut mettre en danger leur liberté d'expression et la démocratie. De plus, l'utilisation de drones pour la surveillance aérienne et le développement de technologies de reconnaissance faciale ont soulevé de nouvelles inquiétudes. Ces outils peuvent aussi présenter des risques importants d'atteinte à la vie privée s'ils sont utilisés sans encadrement strict.
Notamment, dans les villes, les transports, les espaces publics de Chine[15], les caméras de surveillance ne se contentent pas de filmer et de surveiller des individus mais peuvent également alimenter des bases de données massives permettant d'identifier des personnes ou d'associer des comportements à des profils. Ces systèmes peuvent être utilisés à des fins de sécurité publique mais soulèvent également des risques importants en matière de vie privée et de libertés publiques. Éviter d'affirmer sans source solide qu'un système centralisé de surveillance ou de « crédit social » détermine systématiquement l'accès au logement, à l'emploi ou aux prestations publiques.

De plus, certains gouvernements achètent des logiciels espions comme solution de cyber renseignement afin d'espionner des journalistes, des opposants politiques et des militants.

Pegasus est un logiciel espion développé par l'entreprise israélienne NSO Group ; son développement et son utilisation sont documentés dans les années 2010, mais il ne faut pas le présenter simplement comme ayant été créé en 2013 est destiné à attaquer les téléphones afin d'accéder aux fichiers, photos, mots de passe etc… Il a également la capacité d'extraire toutes les données, et même utiliser des photos et applications sans que la personne touchée s'en aperçoive. Pegasus a déployé son logiciel auprès de 40 pays dans le monde. L'utilisation de ce logiciel par les gouvernements peut même conduire à l'élimination des adversaires politiques.

Nombre annuel de demandes de données personnelles de la part d'organismes gouvernementaux dans le monde, de 2013 à 2022 par entreprise

[14] La surveillance abusive : un défi majeur pour nos libertés individuelles | Actus Juridiques
[15] Surveillance en Chine : Regards et Réalités Quotidiennes

Characteristic	Apple	Google	Meta	Microsoft
2013	5,259	85,148	77,774	125,215
2014	9,317	99,202	99,715	111,559
2015	17,322	150,218	123,409	127,364
2016	23,000	150,787	180,613	105,248
2017	55,180	170,644	242,790	85,806
2018	64,045	261,892	322,923	89,118
2019	81,758	340,762	427,858	86,699
2020	84,604	496,633	610,677	96,909
2021	75,550	732,773	716,108	92,161
2022	437,670	839,401	827,927	120,293

User data requests by company 2022| Statista

Ce graphique montre la hausse des demandes de données par des organisations gouvernementales dans le monde.

Comme le volume de données est en constante augmentation, le risque de violation de données est plus élevé. En effet, on peut constater grâce au bilan 2025 de la CNIL, “que le nombre de déclarations de violences de données personnelles a augmenté de 47% par rapport à 2024.” Violations donnees 2025 bilan CNIL

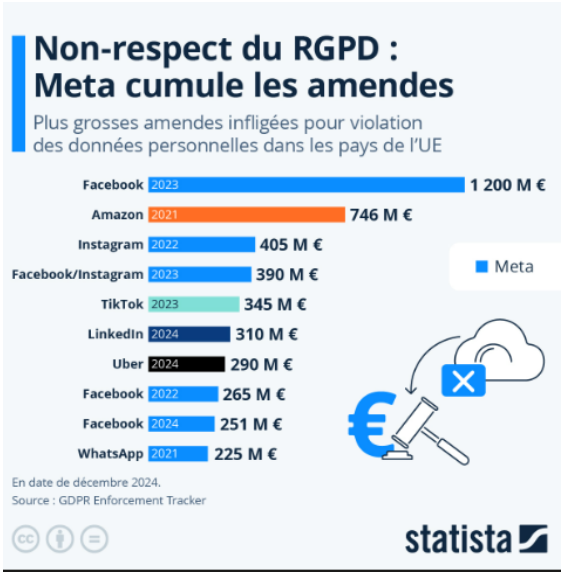
C. Risques de cyberattaques[16]

Enfin, la concentration de grandes quantités de données personnelles chez certains acteurs, dont les data brokers, peut accroître les conséquences potentielles d’une cyberattaque, sachant que ces entreprises sont des cibles privilégiées à des informations sensibles comme l'adresse, le téléphone ou les codes bancaires.
Il existe plusieurs attaques telles que le phishing, utilisant l’usurpation d’identité afin d’obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel. Une attaque par rançongiciel (ransomware) qui bloque l’accès à un appareil ou à des fichiers et réclame le paiement d’une rançon pour obtenir le déchiffrement des données. Et une attaque par un déni de service (DoS)[17] qui est conçue pour interrompre ou arrêter un réseau jusqu’à ce qu’il ne marche plus.

[16] Cybercriminalité : types d’attaques et protection des victimes | info.gouv.fr
[17] Les 15 Types de Cyberattaques les Plus Courantes en 2025 | Trend Micro (FR)

III. Manques de précautions face à la circulation massives des données

A. Les normes existantes présentent encore plusieurs limites



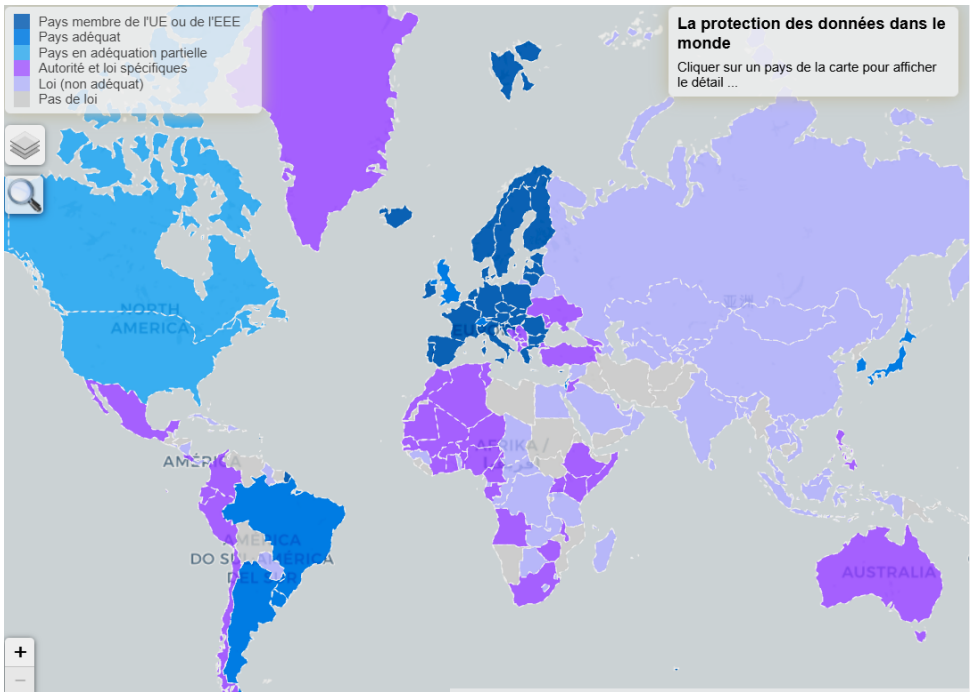
Le **RGPD** et la **Convention 108+** sont deux cadres majeurs de protection des données : le premier est un règlement de l'Union européenne, le second un traité international du Conseil de l'Europe. Le RGPD impose aux organisations de ne collecter que les données nécessaires à leurs services et de garantir des droits aux citoyens. La Convention 108+ fixe des principes communs de protection des données et renforce la coopération entre les Etats.

Cependant, ces normes ne s'appliquent pas partout : le RGPD est limité au territoire de l'UE, et la Convention 108+ n'est approuvée que par un nombre restreint d'Etats. Ainsi, certaines applications provenant de pays non soumis à ces règles peuvent adopter des pratiques de collecte de données moins protectrices, comme le montre le graphique.

B. Des pays ayant aucune normes et sanctions

Selon le conseil des droits de l'homme des Nations-Unis "L'absence de réglementation dans certains pays du monde laisse planer une incertitude quant à la manière de protéger les droits des titulaires de données, voire se traduit par une absence pure et simple de protection contre le traitement inapproprié des données à caractère personnel." International collection of personal data. Effectivement, certains pays disposent d'un cadre juridique limité ou insuffisant pour la protection des données personnelles. Cela cause un problème fondamental pour leur population car elle est exposée à plusieurs risques majeurs déjà mentionnés dans la Partie II.

Les différents niveaux de protection des données des pays dans le monde.



La protection des données dans le monde | CNIL

(cliquer sur la source pour avoir plus d'information sur un pays que vous recherchez)

Synthèse

On assiste à une prolifération des données conduisant dans un monde extrêmement digitalisé. Par conséquent, certains traitements et usages pourraient créer des menaces et générer trois risques majeurs (l'exploitation commerciale, la surveillance étatique et les cyberattaques) . Ainsi, il paraît nécessaire d'encadrer les données afin de limiter ces risques et de faire en sorte que la population continue à bénéficier des progrès apportés par la numérisation.

TRAITÉS DE L'UIT ET GRANDS ÉVÉNEMENTS

28/01/1981

Modernisée en 2018, la **Convention 108+** établit des règles internationales pour protéger des données personnelles. Elle impose des obligations strictes et intègre des principes proches du RGPD. La convention compte 55 Etats Parties avec deux objectifs prépondérants: ”la libre circulation des données et le respect de la dignité humaine”. Convention 108 et Protocoles - Protection des données

1989

La **Coopération économique pour l'Asie-Pacifique** (APEC) vise à faciliter le commerce international et les flux de données entre entreprises. Elle cherche notamment à concilier la circulation des données plutôt que la protection de la liberté individuelle. C’est donc un cadre ouvert au commerce très éloigné des principes de protection des données du RGPD ou de la Convention 108+.

23/11/2011

La Convention de Budapest sur la cybercriminalité est le premier traité international sur les infractions commises via l’Internet et d'autres réseaux informatiques. Elle traite particulièrement, des infractions portant sur les droits d’auteur et sur la fraude informatique. Son principal objectif, énoncé dans le préambule est de poursuivre “ une politique pénale commune destinée à protéger la société contre le cybercrime”. Convention de Budapest - Cybercriminalité

2013, Genève

La **Loi type de la Communauté du développement de l’Afrique australe** (SADC) est un texte modèle conçu pour aider les Etats d'Afrique australe à créer leur propre réglementation sur la protection des données personnelles. Titre du rapport comme le déclare l’UIT, l’objectif de cette loi type est “de combattre les violations de données susceptibles de découler de la collecte, du traitement, de la transmission, du stockage et de l’utilisation de données à caractère personnel.” De plus, la loi modèle SADC met en évidence une transparence de la circulation des données personnelles, qui ne doit jamais être de manière abusive et cachée.

03/2018

Le **CLOUD Act** est une loi américaine qui permet aux autorités d'accéder aux données, même stockées à l'étranger. Il renforce la surveillance étatique et crée des tensions avec les normes internationales de protection de données. CLOUD Act — Wikipédia

25/05/2018

Le **RGPD** (Règlement Général sur la Protection des Données) est le cadre juridique européen qui encadre la collecte, l'usage et la protection des données personnelles. Ce règlement vise à garantir un haut niveau de protection pour les personnes et à imposer des obligations strictes aux organisations. Le RGPD est très important car il permet aux citoyens d'exercer davantage de droits et de contrôle sur leurs données.

10/07/2023

Le **Cadre de Protection des Données (DPF)** est un mécanisme juridique qui permet le transfert de données personnelles de l'Union Européenne vers les États-Unis. Il n'impose pas aux entreprises américaines des règles identiques au RGPD. Le Data Privacy Framework permet notamment des transferts de données vers les organisations américaines participantes dans le cadre de la décision d'adéquation de l'Union européenne et prévoit des garanties spécifiques. Ainsi, il sert à protéger les données européennes tout en permettant la circulation vers les Etat Unis.

SOLUTIONS POSSIBLES

→ Encourager l'instauration d'un règlement universel par les institutions internationales, pour tous les pays afin d'assurer une protection commune.

→ Adopter un partenariat et des règles avec les Etats Unis (et d'autres grandes puissances technologiques) étant donné qu'ils sont les précurseurs et les plus développés dans ce domaine au travers des GAFAM et de l'AI (Anthropic, et Open AI).

→ Les institutions internationales peuvent formuler une recommandation prévoyant une augmentation des sanctions pour le non-respect des lois sur la protection des données.

→ Homogénéiser les principes et traités majeurs pour créer un règlement commun à tous. Par exemple s'assurer que des réglementations de type RGPD soient implémentées dans tous les pays du monde.

QUESTIONS GUIDÉES

Comment les institutions internationales peuvent-elles imposer des règles communes dans un monde où les législations nationales sont très différentes ?

Le modèle européen (RGPD, Convention 108+) peut-il coexister avec des modèles plus souples comme celui de l'APEC ou plus intrusifs comme le CLOUD Act ?

Les mécanismes actuels de coopération (Convention de Budapest) sont-ils assez efficaces pour protéger les données contre les cybercriminels?

Comment empêcher les Etats d'utiliser les données pour une surveillance abusive tout en leur permettant de lutter contre la criminalité ?

Les institutions internationales peuvent-elles réellement encadrer les data brokers alors que leur activité est globale et souvent opaque?

BIBLIOGRAPHIE

Article de presse et site web

Données personnelles :

- People must know what data is generated and processed | Privacy International
- Donnée personnelle ou donnée à caractère personnel définition - Definition-juridique.fr

Institutions internationales :

- Les institutions internationales | Secondaire | Alloprof
-

Exploitation commerciale :

- https://www.legifrance.gouv.fr/codes/section_lc/LETEXT000005634379/LEGISCTA000006179001/?utm
- Data Brokers : un marché opaque au cœur des menaces informationnelles - Semkel

Entreprises classiques:

- Demandes de crédit : comprendre l'utilisation de vos données et vos droits | CNIL

Surveillance abusive:

- Edward Snowden, un lanceur d'alerte déterminé | INA
- Le FBI achète les données de géolocalisation des citoyens US : et en France ?

- Logiciel espion:Pegasus (logiciel espion) — Wikipédia Pegasus : le logiciel espion le plus dangereux jamais créé
- Surveillance de masse Chine:Surveillance en Chine : Regards et Réalités Quotidiennes

Big data :

- Big Data : définition, technologies, utilisations, formations
- GAFAM — Wikipédia

Data brokers:

- Courtiers en Données : Qui Vend Vos Infos Personnelles ?
- Data Brokers : un marché opaque au cœur des menaces informationnelles - Semkel

Niveau de protection dans le monde:

- La protection des données dans le monde | CNIL

Rapports

Rapports institutions internationales:

- ITU Data Protection and Privacy Policy
- Collecte des données ONU International collection of personaldata:
- ONU manque de réglementation International collection of personal data

Rapport diverses:

- Loi Communauté SADC Titre du rapport
- Convention 108+ Convention 108 et Protocoles - Protection des donnée
- Convention de Budapest Convention de Budapest - Cybercriminalité

L'étude sur le Cloud protection des données:

- GSR12Contribution_forinfo_TunisieTelecom.pdf

Video

vidéo sur le big data:

- Le big data - 60 secondes pour comprendre