C11- Aspects réglementaires sur l’utilisation des données et des logiciels

Introduction

- La collecte et le traitement des données par des organisations vont croissants.
- Le législateur s'adapte en conséquence.
- Garantir la liberté des personnes
- S'assurer de la nature et de la sécurité des données.
- Poser des obligations pour les organisations utilisant et traitant les données

Introduction

- Risque de hacking sur les données collectées par les organisations.

- 2018 : "Google : les données de 500 000 utilisateurs touchées par une faille"
  Lien / article de Siècle Digital

- 2018 : "Faille Facebook, des données de 29 millions de comptes récupérées par les pirates"
  Lien / article du Monde

- Les exemples sont nombreux :
  Lien / article lebigdata.Fr

Introduction

Collecter et traiter des données, un risque pour la liberté et les droits des personnes ?

Se voir refuser un prêt ou une mutuelle parce qu'une banque a pu obtenir des informations sur sa santé

Voir des aspects de sa vie personnelle ou intime dévoilée du fait des sites web visités

Une embauche ne se fait pas parce qu'on a repéré que le candidat est communiste, syndiqué, juif ou musulman

Des élections qui se retrouvent influencées par les réseaux sociaux. Liberté de choix lorsque certaines informations sont tues et d'autres sur-mediatisées ?

Une embauche ne se fait pas parce que le candidat a exprimé il y a 20 ans des opinions racistes

Utilisation de la géolocalisation pour savoir qui est avec qui, quels maris / femmes trompent leurs maris / femmes…

Introduction

Risque principal sur **le recoupement des données**

Introduction

- Dans certains cas, on pourrait débattre.
- Une banque cherche à obtenir plus d'information sur la santé des emprunteurs : aspects positifs et négatifs ?
- Le fait de connaître les préférences des individus en matière politique : aspects positifs et négatifs ?
- Connaître le passé judiciaire des individus : aspects positifs et négatifs ?

Introduction

Des cas qui ont fait / font débat :

- Poupées Barbie qui enregistrent les conversations, les envoient sur les serveur de Matel (février 2015)
- Nouvelle-Zélande : récupération de données sur les enfants pour identifier les profils d'enfants "à risque" (2017). Lien / bigdata.fr
- Le cas de salariés licenciés pour avoir tenu des propos désobligeants sur leur entreprise sur Internet. Lien / cas de 2010, Lien / cas de 2011

Introduction

- Chaque personne ou organisation peut se considérer comme collectant et traitant des informations

- Chaque personne ou organisation peut considérer les données qui sont collectées, conservées et utilisées sur elle.

Introduction

- Les Etats investissent ce nouveau champ du droit.

- La France a été précurseure avec la CNIL, le 06/01/78, modifiée en 2004. La CNIL : une Loi et une autorité instaurée par la Loi.

- 2016 : **Règlement Général sur la Protection des Données**, règlement européen. Entrée en vigueur le 25 mai 2018. En France, la CNIL est l'autorité souveraine de mise en application du RGDP.

Introduction

- Le 21/03/1974, un article du Monde revèle le projet SAFARI.
- SAFARI = Système automatisé pour les fichiers administratifs et le répertoire des individus.
- Volonté d'interconnecter tous les fichiers nominatifs grace au numéro INSEE et donc de pouvoir tout connaître sur les personnes.
- Forte opposition de l'opinion, le projet est abandonné.
- Loi CNIL en 78, une loi similaire avait vu le jour en Allemagne dans les 70s

Introduction

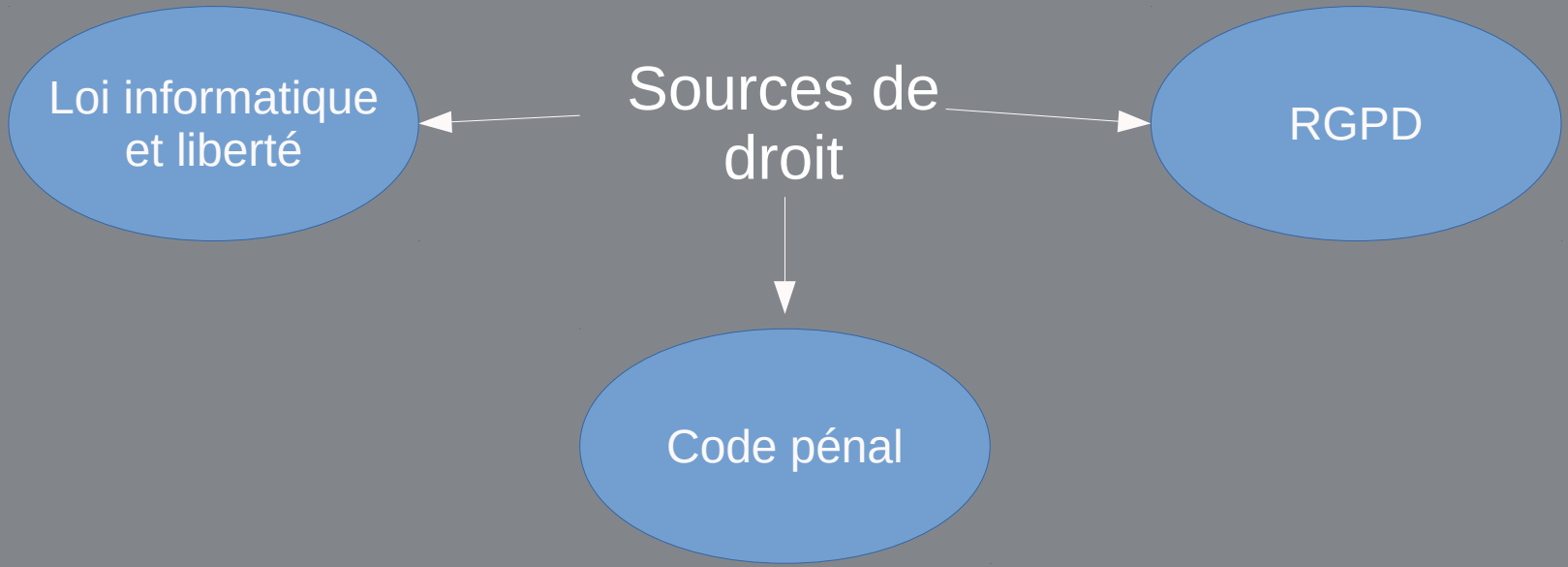
Début de l’Article 1 de la loi informatique et libertés :

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Introduction

- La problématique de la protection des données et du droit sur les logiciels est de plus en plus prégnante
- Un droit de propriété qui a vocation à évoluer.
- De nouveaux délits qui apparaissent / sont apparus.

Introduction



Plan

1) RGPD

2) Mise en conformité avec le RGPD

2) Droit sur les logiciels et les contenus

3) Evolution du code pénal

Les grands principes 1/2

- Les organisations doivent offrir une information claire, intelligible et aisément accessible sur le traitement des données qu'elles font.
- Nécessité de donner un consentement ou de pouvoir s'opposer au traitement de ses données personnelles.
- Charge de la preuve du consentement qui repose sur le responsable du traitement.
- Droit à la portabilité et à la limitation des données personnelles.

Les grandes principes 2/2

- Possibilité de recours collectifs, droit à la réparation des dommages matériels ou moraux
- Responsabiliser les entreprises.
- Allégement des formalités préalables (déclarations et autorisations) VS responsabilisation des entreprises
- Tenue d'un registre des traitements dans certains cas, notification des failles de sécurité, nomination d'un délégué à la protection des données (DPO*), études d'impact sur la vie privée.

*Data Protection Officier.

Données à caractère personnel

- Depuis le site de la CNIL : "toute information se rapportant à une **personne physique** identifiée ou identifiable"

- En font partie : une photo, le nom, une empreinte, une adresse postale, un mail, un téléphone, une adresse IP, un enregistrement vocal, une plaque d'immatriculation…

- Des données comme l'age, le sexe, le diplôme, … sont considérées comme personnelles si elles permettent d'identifier une personne

Données sensibles

- Les article 9 et 10 du RGPD déterminent les données sensibles
- Leur traitement peut présenter des risques pour les individus.

- Opinions politiques
- Appartenance syndicale
- Convictions religieuses ou philosophiques
- Orientation sexuelle ou données sur la vie sexuelle
- Origine raciale ou ethnique
- Les données sur la santé
- Données génétiques ou biométriques
- Les condamnations pénales, infractions et mesure de sûreté.

Données sensibles

- A noter que les données sensibles concernent les individus
- Une entreprise peut avoir des données dites sensibles (secrets de fabrication, chiffres stratégiques…) ...
- … mais la notion de données sensibles du RGPD ou de la CNIL concerne les personnes.

RGDP et données sensibles

La règlement européen interdit de **recueillir** ou d'**utiliser** des données à caractère personnel, sauf dans certains cas :

- Si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée)
- Si les informations sont rendues publiques par la personne concernée
- Si elles sont nécessaires à la sauvegarde de la vie humaine et que la personne est dans l'incapacité de donner son consentement.
- Si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL (santé, police, traitement d'un arrêt de travail...)
- Traitement dans le cadre d'associations ou organismes à but non lucratif si les DCP ne sortent pas de l'organisme (association, parti politique, syndicat ...)

Le consentement

- Libre
- Spécifique
- Éclairé
- Univoque
- Facilement révocable

Traitement des données personnelles

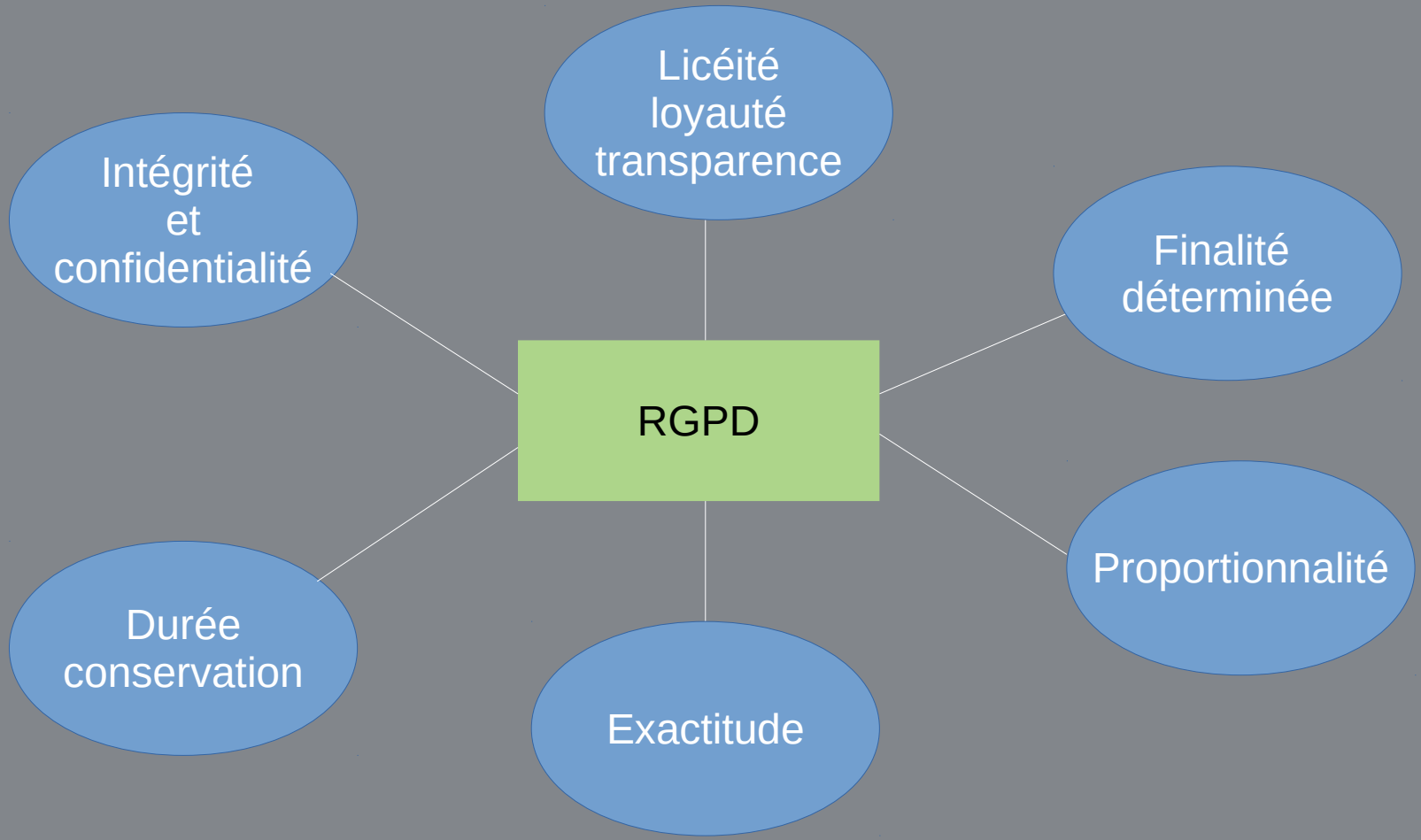
DEF : toute opération ou tout ensemble d'opérations effectuées
ou non à l'aide de procédés automatisés et appliqués à des données
à caractère personnel, telle que la collecte, l'enregistrement, l'organisation ,
la structuration, la conservation,
l'adaptation ou la modification, l'extraction, la consultation,
l'utilisation, la communication par transmission,
la diffusion ou toute autre forme de mise à disposition,
le rapprochement de l'interconnexion,
la limitation, l'effacement ou la destruction.

Des exemples de traitements ?

Principe de privacy by design

- Protection des données dès la conception ou par défaut.
- Article 25 du règlement.
- Les outils, produits, application ou services offerts aux clients doivent intégrer dès leur conception et de façon effective les principes relatifs à la protection des données et par défaut, ces outils, produits, applications ou services doivent garantir que seules sont traitées **les données nécessaires à la finalité du traitement**.

Les principes du RGPD



Licéité, loyauté, transparence du traitement (1)

- Tout traitement doit avoir une finalité autorisée.

- L'article 5 du RGPD indique les conditions de licéité d'un traitement.

Licéité, loyauté, transparence du traitement (2)

L'une des conditions suivantes doit être remplie :

* La personne concernée a consenti au traitement de ses données pour une ou plusieurs finalités spécifiques
* Le traitement des données est nécessaires à l'exécution d'un contrat auquel la personne concernée est partie
* Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis.
* Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.
* Le traitement est nécessaire à l'éxécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement
* Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par les responsables du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui

Finalité du traitement

- Pour tout traitement, l'organisation doit définir sa finalité.
- La finalité doit être déterminée, explicite et légitime.
- Les organisations ne sont pas censées faire de détournement de finalité avec les données.
- Des exemples de détournement de données ?

Minimisation des données

- Les données collectées doivent être adéquates, pertinentes et limitées strictement à ce qui est nécessaire au vu des finalités.

- Cela s'applique aussi aux données qui sont transmises aux sous-traitants.

Limitation de la conservation

- Limitation de la durée de conservation aux seules données personnelles nécessaires au traitement.

- Au delà : destruction ou anonymisation.

Limitation de la conservation

- La loi française précise des limites de conservation. Des exemples divers.
- Données relatives à la gestion du personnel => 5 ans (Selon Art R.1221-26 du Code du travail)
- Conservation de même durée pour les bulletins de paie.
- Données de vidéosurveillance, 1 mois de conservation au max (Art L.252-3 du Code de la sécurité)
- Dans le cas où la Loi ne précise pas → le responsable des traitements doit le faire.

Protection particulière de certaines données

- Sont concernées les données particulièrement sensibles du point de vue des libertés ou des droits fondamentaux

- Sont concernées :
  - Les données sensibles

  - Le numéro de SS (un décret du Conseil d'État détermine les organismes habilités à traiter le NIR : Pole Emploi, employeurs, professionnels de santé, organismes de SS...)

  - Les données personnelles relatives aux condamnations pénales, aux mesures de sécurité, aux infractions.

Obligation de sécurité

La sécurité s'apprécie en fonction de la sensibilité des données.

Droits des personnes sur leurs données

- Droit d'accès, droit d'opposition, droit de rectification, droit au refus du profilage ou de décisions automatisés, droit à la limitation du traitement.
- Droit à la portabilité des données (art. 20)
- Droit à l'effacement (art. 17). Précédemment nommé "droit à l'oubli" dans la CNIL.

Evolution de la CNIL avec le RGPD

- La CNIL ne disparaît pas.
- Autorité qui contrôle et accompagne dans l'application du RGPD, informe le grand public
- Capacité d'intervention étendue.

CEPD

Centre Européen sur la Protection des Données

Institué par l'article 29 du RGPD

Veille à l'application du RGPD, notamment dans les organes européens.

Plan

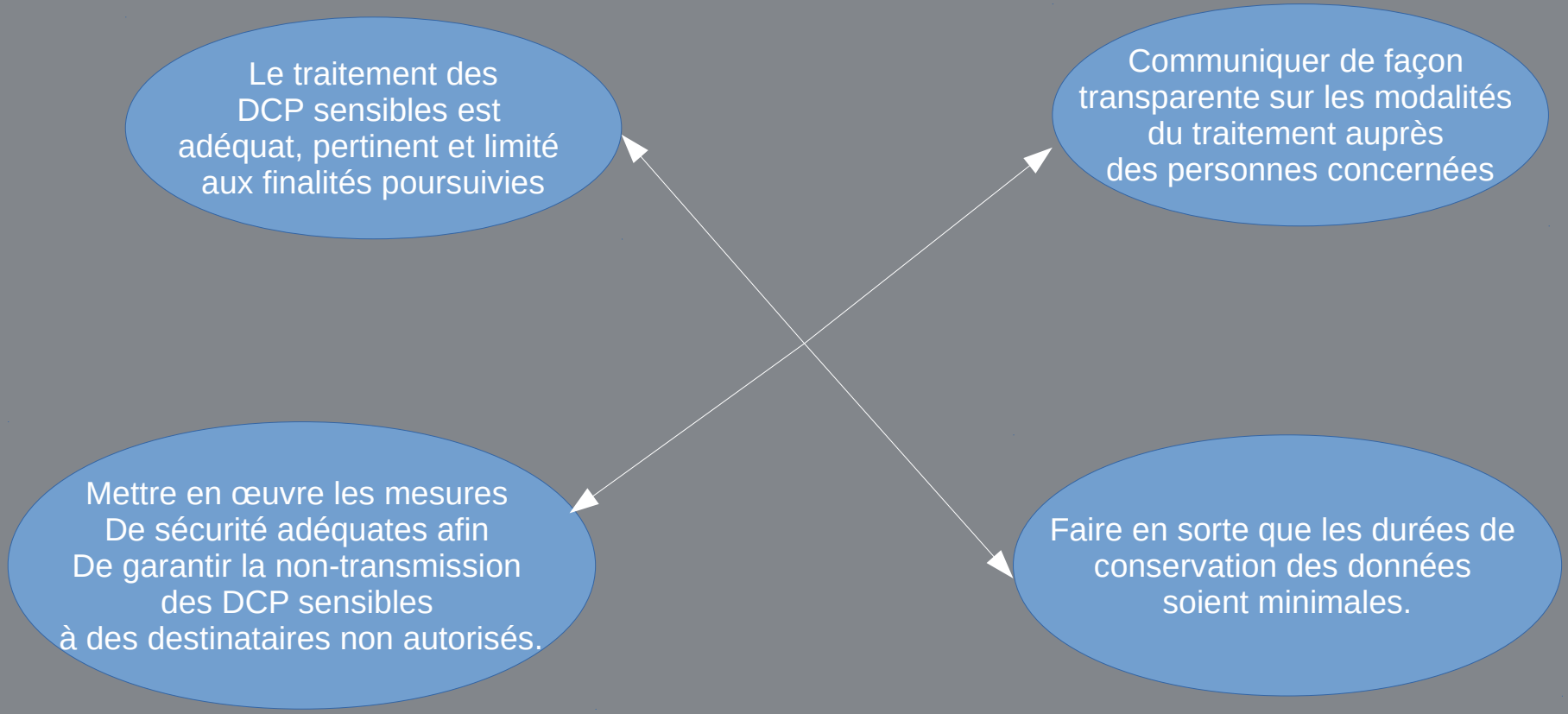
1) RGPD

2) Mise en conformité avec le RGPD

3) Droit sur les logiciels et les contenus

4) Evolution du code pénal

Mise en conformité



Mise en conformité

- Les organisations collectant des données doivent mettre en place une protection optimale des données.

- Les organisions doivent documenter leur mise en conformité afin de la démontrer au besoin. Principe d'accountabiliy

Mise en conformité - DPO

- DPO : obligation pour les organisations de plus de 250 salariés.

- Rôle et qualité :
  - Informer et conseiller les responsables des traitements
  - Contrôler le respect du règlement
  - Conseiller l'organisme
  - Coopérer avec l'autorité de contrôle et être le point de contact.

Mise en conformité - Registre

- Obligation de registre pour tout organisme qui traite de données personnelles.

- Le registre répertorie tous les traitements des données personnelles en respectant le principe d'accountabiliy.

Mise en conformité – Autres aspects

- AIPD : analyse d'impact relative à la protection des données.
- Prioriser les actions
- Audit technique
- Plan d'actions

Mise en conformité – Temps de conservation

- Article de référence : sur le site de la CNIL

- Un principe à retenir : hors des définitions légales de conservation, la conservation se fait fonction de la finalité des traitements.

Des condamnations au RGPD

- Lien sur le site PLRAvocats.
- Lien sur le site de la CNIL.
- Une condamnation d'Amazon.
- Le rapport d'activité de l'autorité belge de protection des données
- Sur le site de l'ordre des EC en 2020, les premiers retours.

Des condamnations au RGPD

- 10 millions d’euros ou 2% du chiffre d’affaires : c’est le cas lorsque les entreprises violent les conditions imposées concernant le recueil du consentement des enfants ou si elles ne respectent pas le principe du privacy by design ou du privacy by default.

- 20 millions d’euros ou 4% du chiffre d’affaires : c’est le cas lors d’une violation des principes de traitement des données ou le non-respect des conditions de licéité du traitement.

Plan

1) RGPD

2) Mise en conformité avec le RGPD

3) Droit sur les logiciels et les contenus

4) Evolution du code pénal

Propriété intellectuelle

- La loi de 1957 protège "toutes les œuvres de l'esprit, quels qu'en soit le genre, la forme d'expression, le mérite ou la destination" article 2.

- Cela concerne les écrits littéraires, artistiques, scientifiques, le cinéma, la musique….

Propriété intellectuelle

- Loi de 1985 qui étend la protection, notamment aux programmes informatiques.
- Loi de 1992 qui abroge les lois de 57 et 85 et les intègre dans le Code de la Propriété Intellectuelle.
- 1993 : directive européenne harmonisant le droit d'auteur à 70 ans après le décès de l'auteur.

Dépôt d'un brevet

- La conception du logiciel n'est pas protégée (idée, principe, algorithme…)
- Ce qui peut être protégé : les programmes, architectures, écrans, documentation.
- Dépôt possible notamment auprès de l'INPI.

Licences – Quelques considérations

- Licence par poste, licence globale…
- Licences du libre
- Licence creative commons

Plan

1) RGPD

2) Mise en conformité avec le RGPD

3) Droit sur les logiciels et les contenus

4) Evolution du code pénal

Délinquance informatique

- La délinquance informatique a fait son apparition : Loi Godfrain de 1988, qui ajoute un chapitre au Code Pénal
- **Accès frauduleux à un système informatique**. Sanctions : 2 ans d'emprisonnement et 30 000 € d'amende. Cela comprend également les accès commis par jeu et défi.
- **Altération volontaire de systèmes informatiques**. Sanctions : 5 ans d'emprisonnement et 75000 € d'amende.
- **Altération volontaire de données**. Sanctions : 5 ans d'emprisonnement et 75000 € d'amende.
- **Tentative de fraude et fraude en association**. Pour ces tentatives, le délit est puni autant que la tentative.

Conclusion / débats

- Amende de 50 millions d'€ à Google de la CNIL le 28 janvier 2019 "pour manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité."
- Des principes non encore pris en compte par la loi : neutralité du net.
- Notion de service universel
- Vers de nouvelles formes de propriétés ? De nouvelles applications (vote en ligne, Primaire.org)