INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

INFORMATIQUE ET CADRE JURIDIQUE
UN TOUR EN 90 MINUTES?

Frédérique BIENNIER

MOTIVATIONS

- Information
  - 3eme dimension après
    - La matière
    - L'énergie
  - Evolution sur le traitement de l'information
    - Artisanat
    - Industrialisation
    - Cycle raccourci par rapport à la révolution industriel
- Informatique c'est
  - Le matériel dans les années 50
  - Le logiciel dans les années 70
  - Le service associé dans les années 2000
- Une technologie et des usages
  - Protéger et rentabiliser les innovations technologiques
  - Création d'un monde virtuel

CADRE JURIDIQUE, DROIT… ESSAI DE DÉFINITION

- C'est quoi
  - Ensemble de règles moralement neutres
    - Règlements (arrêtés): produits par des exécutifs
    - Lois: votées cadre législatif
  - Différents cadres
    - Cadre fondamental
    - Cadre normatif
    - …
- Ca sert à quoi
  - Définir des règles régissant les relations entre personnes dans une société
    - Inclusion des activités commerciales
  - Permettre de définir un vivre ensemble juste
  - Protéger la souveraineté
- Ca a des limites d'application
  - Territorialité vs extraterritorialité
  - Universalité

Frédérique BIENNIER

3

- **PROTECTION INDUSTRIELLE**
  - Quel cadre pour quel besoin
  - Droit d'auteur
  - Logiciel libre et open source
- **PROTECTION DES USAGES: FOCUS SUR LES DONNÉES PERSONNELLES**
- **LÉGISLATION ET SOUVERAINETÉ NUMÉRIQUE**
- **POUR CONCLURE…**

Frédérique BIENNIER

4

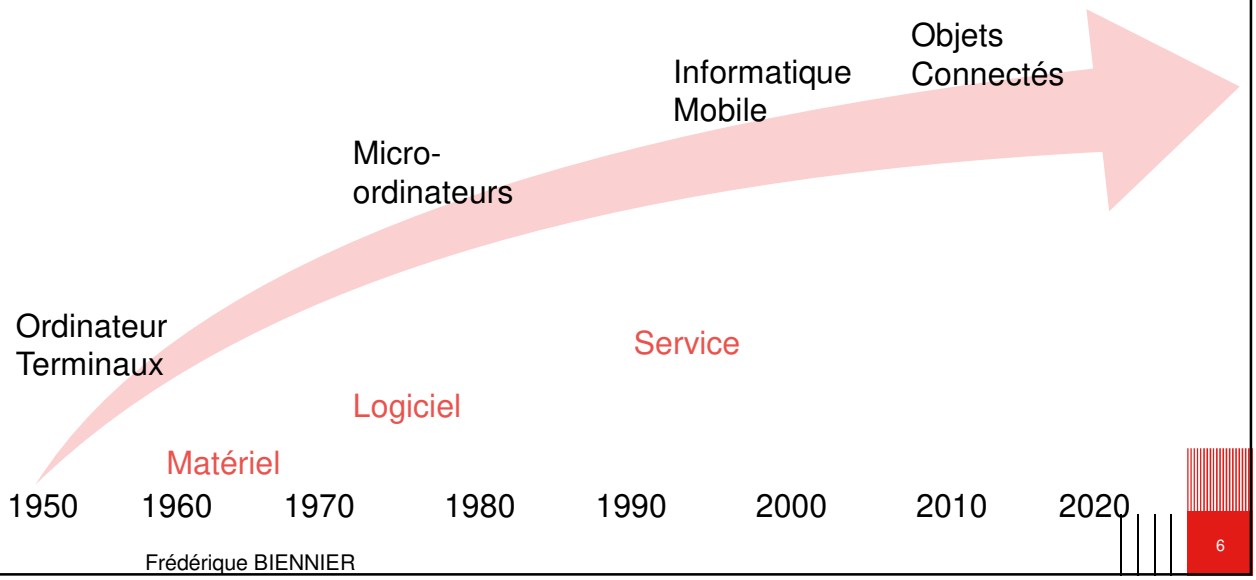
CADRE JURIDIQUE, DROIT… ET OBJETS TECHNOLOGIQUES

- Objet technologique
  - Tangible
  - Intangible
- Pourquoi?
  - Protection industrielle
    - Brevets
    - Droit d'auteur
  - Protection de la société
    - Impacts possibles
    - Réguler les usages
      - Danger pour les personnes
      - Remise en cause des fondamentaux du vivre ensemble
        - Ethique

Frédérique BIENNIER

5

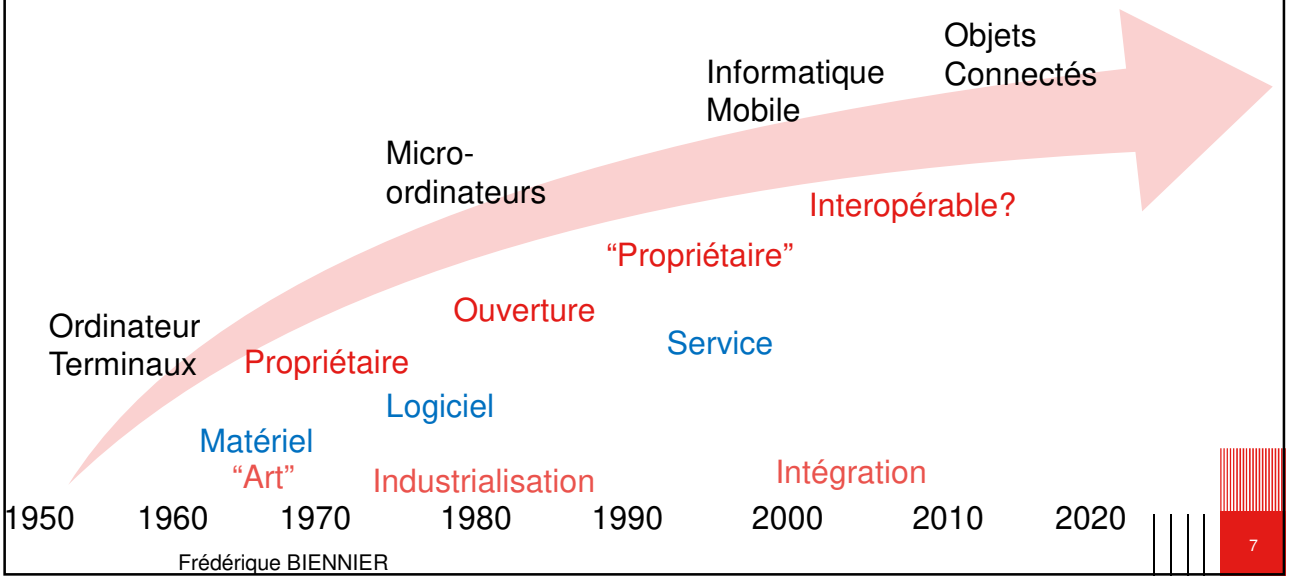
QUEL CONTEXTE POUR L'INFORMATIQUE?



Frédérique BIENNIER

6

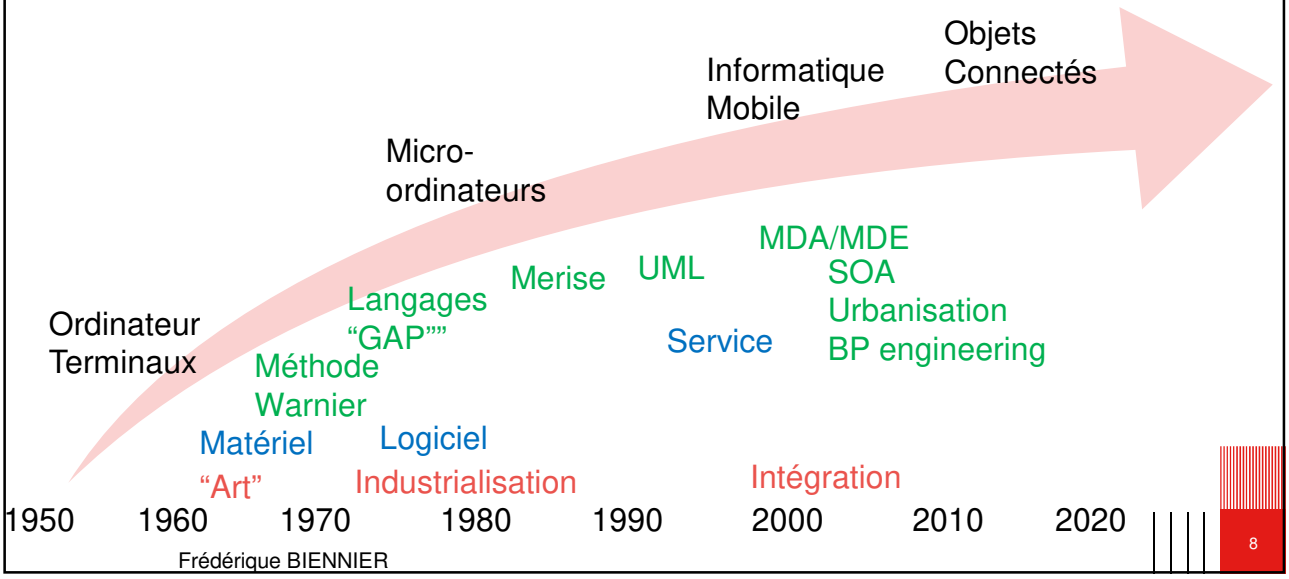
QUEL CONTEXTE POUR L'INFORMATIQUE?



Frédérique BIENNIER

7

QUEL CONTEXTE POUR L'INFORMATIQUE?



Frédérique BIENNIER

8

EVOLUTION DES BESOINS

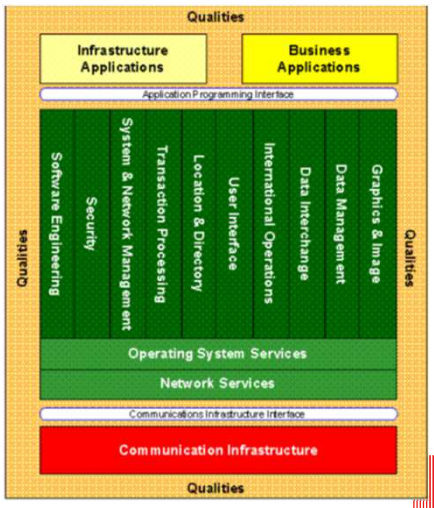
- Années 60 - 70:
  - Programmation artisanale
  - Coûts de possession élevés
  - Développements concernant les langages, BD, systèmes de fichiers…
  - Logique de production informatique « industrielle »
  - Explorations vers le multi-média…
- Années 80 - 95
  - BD relationnelles -> ouverture possible
  - Programmation objet
  - Progiciels et offres « sur étagère »
  - Première phase d'industrialisation de la production logicielle
- Années 95 / 2000
  - Progiciels à large échelle
    - Coût d'achat mineur
    - Large part de coûts de « paramétrage »
  - Environnements « propriétaires »
  - Développement de « frameworks »
  - Industrialisation de la production logicielle
- Depuis 2000
  - Mutation vers un environnement de services
  - Baise des coûts de communication
  - Logique de middleware
  - Pay per use
  - Développement du logiciel libre
  - IoT
  - …

INFORMATIQUE, UN PRODUIT « INDUSTRIEL »? (1)

- Production de masse ou production unitaire?
  - Matériel
    - Production unitaire « de luxe » dans les années 60-70
    - Production de masse avec l'arrivée des PC
    - Loi de Moore
      - Limite sur des pbs « thermique »
      - Organisation du parallélisme
      - Mainframe basés sur des PC!
    - Baisse du coût de possession
  - Logiciel
    - Années 60-80: Développement monolithique à façon
    - Production « de masse »: progiciels et produits sur étagère
    - Architectures en couches
      - Réutilisation
      - Personalisation

INFORMATIQUE, UN PRODUIT « INDUSTRIEL »? (2)

- Production unitaire?
  - Architectures en couches
    - Logique de postponent
      - Différenciation retardée
      - Réutilisation de parties « cœur » commune
    - « Standards »
      - Interface
      - Méthodes
  - Capitalisation dans des frameworks
  - Différenciation des prestations
  - Architecture?
    - Intégration de composants
    - Penser le cycle de vie complet
      - DevOps



INFORMATIQUE, UN PRODUIT « INDUSTRIEL »? (3)

- Mutation des modèles de coûts
  - Phase 1: Matériels vs logiciel
    - Achat de temps machine
  - Phase 2: matériel + logiciel vs exploitation
    - Propriétaire
    - Tendance vers l'externalisation de l'exploitation (TMA et télémaintenance)
  - Phase 3: matériel + logiciel vs service apporté
    - Développement des modèles basé sur le logiciel libre
    - Attention aux licences GPL
    - Choix politique industrielle
  - Phase 4: Pay per use
    - Retour au modèle des années 70
    - Achat usage machine + logiciel
    - Possible via la logique de personnalisation « en couches »
  - Phase 5: Architecture diffuse et distribuée?
- Identifier le produit
  - Ce qui apporte de la valeur!

PROTECTION INDUSTRIELLE

- Objectif
  - Pérénizer des savoirs industriels
  - Garantir un droit d'exploitation
  - Brevet
    - Protéger une innovation dans un domaine technique impliquant « 'usage contrôlé des forces de la nature »
    - Impose un lien avec la physique
    - Exclusion de fait du vivant et des mathématiques
- Définition de l'INSEE
  - Le brevet protège une innovation technique, c'est-à-dire un produit ou un procédé qui apporte une solution technique à un problème technique donné. L'invention pour laquelle un brevet pourra être obtenu doit également être nouvelle, impliquer une activité inventive et être susceptible d'application industrielle.
  - De nombreuses innovations peuvent faire l'objet d'un dépôt de brevet, à condition de répondre aux critères de brevetabilité et de ne pas être expressément exclues de la protection par la loi
  - Certaines inventions ne sont pas brevetables mais peuvent faire l'objet d'autres types de protection, comme le droit d'auteur ou le dépôt de dessins et modèles

QUE RECOUVRE LE DROIT D'AUTEUR POUR L'INFORMATIQUE?

- Le droit d'auteur s'applique à la totalité d'une oeuvre
  - Les modèles
    - Données
    - Processus
  - Le logiciel
    - Code
    - Données manipulées
- Jurisprudence:
  - Les données du SI "appartiennent" à l'auteur du logiciel
    - Le modèle de données est une part de l'oeuvre
    - Contrôle des usages
  - Peut s'opposer à la portabilité des données?
    - Limitation de ce droit pour les données personnelles

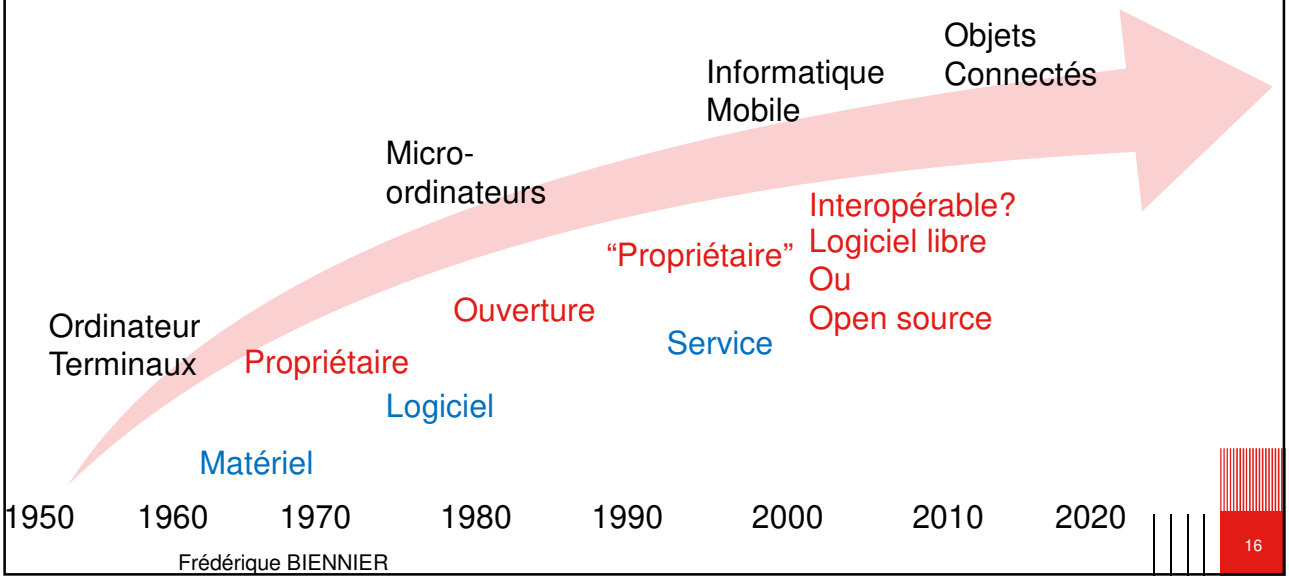
DROIT D'AUTEUR ET PROTECTION LOGICIELLE

- Différences avec les autres types d'oeuvres
  - Droit à la copie pour usage privée?
  - Intégration du contrôle d'usage
    - Différentes conditions
    - Prise en compte des "modifications"
- Prouver l'antériorité
  - Conserver une trace datée => Envoi d'un recommandé conservé scellé
  - Remise du pli à un tiers type officier ministériel
  - Sites spécialisés
    - Service d'enregistrement et de dépôt comme app
    - Contrôle du code similaire au contrôle anti-plagiat
    - Modèle économique impliquant abonnement et dépôt (different du brevet)

Frédérique BIENNIER

15

QUEL CONTEXTE POUR L'INFORMATIQUE?

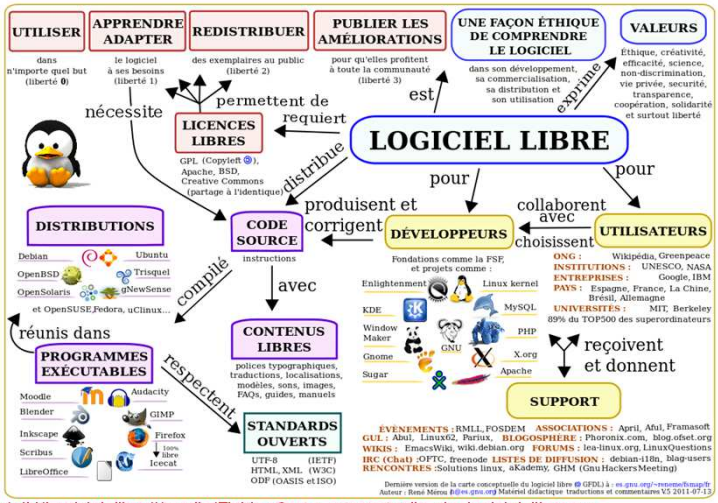


Frédérique BIENNIER

16

LOGICIEL LIBRE?

- Définition de la Free Software Foundation en 1986
  - Partage
    - Liberté de copier le logiciel
    - Liberté de redistribuer le logiciel (en mode gratuit ou non)
  - Contrôle du logiciel
    - Liberté d'étudier le logiciel
    - Liberté de modifier le logiciel
- Logiciel Open Source
  - Permet l'accès au code
  - Droits attachés à la licence (open source ne veut pas dire logiciel libre)
- Gratuité?
  - Pas seulement pour un logiciel libre!
  - Quel est le produit?



Source: https://fr.wikipedia.org/wiki/Logiciel_libre#/media/Fichier:Carte_conceptuelle_du_logiciel_libre.svg
Par René Mérou [h(at)es.gnu.org] and this list of authors related to the icons in http://es.gnu.org/~reneme/fsmap/fsmap-contents.svg : Rubén Rodríguez Pérez, Sun Microsystems, Hitflip team, Ricardo Fernandez Fuentes, David Vignoni, User: Aurelio A. Heckert, (Larry Ewing, Simon Budig and Anja Gerwinski), Agnieszka "pixelgirl" Czajkowska, Frédéric Bellaiche, Sven (Wikipedia), Everaldo Coelho, Ruud Kuin, Nicolas P. Rougier, The Oxygen Team, The GIMP art/developer team, David Šebík, Gryn Frøiland and Håvard Frøiland, Scribus team, Yug, Tango-artists, GNUX Art, 'Cathbard Druid', Joshua "Jag" Ginsberg and the Apache Software Fundation. For this and the Gnome theme extras follow that link for more details. — http://es.gnu.org/~reneme/fsmap/fr/fsmap-fr-w.svg, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=11404067

PETIT RAPPEL SUR LES LICENCES DU LOGICIEL LIBRE

- BSD
  - Logiciel libre pouvant être réutilisé sans restriction
  - Avec ou sans mention de copyright (lourd selon le nombre de composants)
  - Non copyleft => les réutilisations ne sont pas soumises à l'obligation de rester libre
  - Protection des noms des auteurs sur les produits dérivés
- Apache
  - Logiciel libre et open source
  - Obligation de mentionner le copyright pour tous les composants
  - Non copyleft
  - Maintien des NOTICE
- GNU GPL
  - Copyleft => les modifications / extensions doivent être diffusées
  - « Droits » vs liberté: permet l'analyse et la modification du code mais oblige à rester dans le même contexte
  - Version permettant la cohabitation avec le logiciel propriétaire

QUEL MODÈLE INDUSTRIEL POUR LE LOGICIEL LIBRE

- Diffusion du code
  - Préservation de la propriété intellectuelle
  - Contrôle sur les évolutions selon les licences
- Changement de modèle économique
  - Service vs produit
    - Jours/homme
      - Intégration
      - Support
    - Contrôle des évolutions / corrections
  - Ecosystème et communauté
    - Rôles différents
    - Nouvelle gouvernance?

GOUVERNANCE DANS LE DOMAINE DE L'OPEN-SOURCE

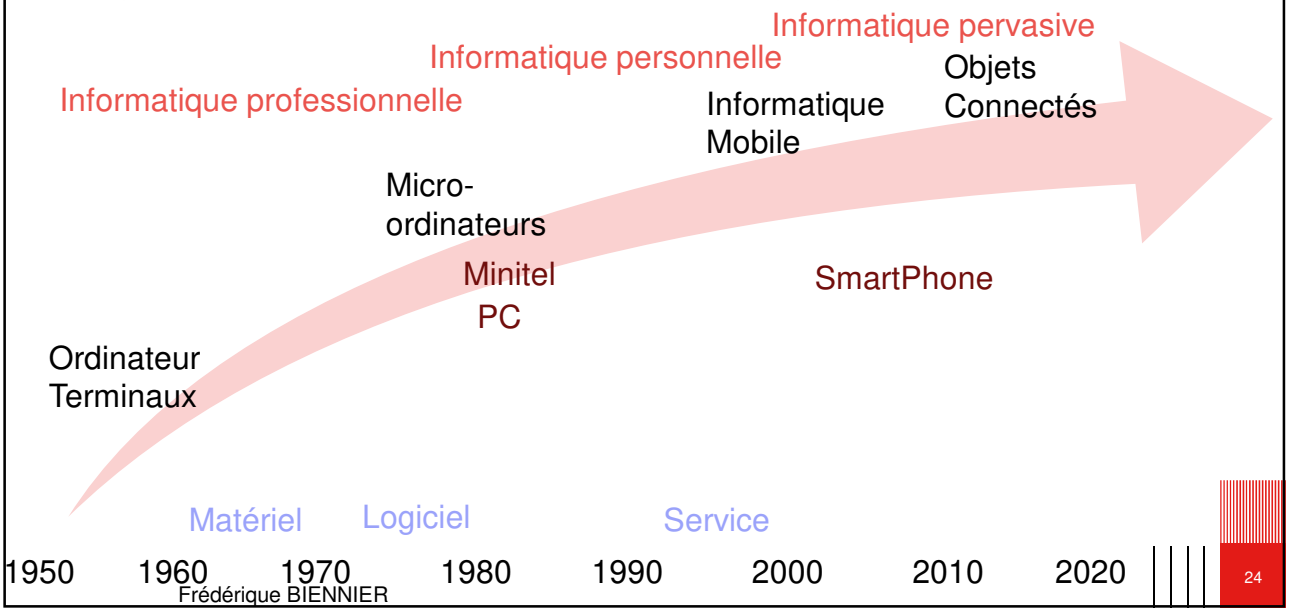
- Cycle de vie des produits open source
  - « Étape d'innovation »
    - Définition du produit logiciel et développement de base
    - Communauté réduite
    - « Gouvernance spontanée »
  - Étape de développement
    - Développement complet et amélioration continue du logiciel
    - Augmenter le nombre de membres de la communauté
    - « Gouvernance interne »
  - Maturité du produit
    - « Services supplémentaires »
    - La communauté est reconnue
    - « Gouvernance vis-à-vis des parties extérieures »
    - Différentes exigences et règles de gouvernance

STRATÉGIES DE GOUVERNANCE DANS L'OPEN SOURCE

- Do-ocracy
  - Qui fait le travail prend la décision
  - Pas de gouvernance formelle
- Piloté par le(s) member(s) fondateur(s)
  - Les contributeurs initiaux ont géré les décisions
  - Contrôle total sur la vision et les modifications de code
- Conseil / conseil auto-désigné
  - Différents groupes pour gérer différents types de décision
  - Répartition claire des sujets de gouvernance (architecture, comité technique, comité de pilotage)
- Basé sur le vote
  - Élection des candidats pour définir les décisions d'organisation
  - Choix pour les modifications logicielles
- Géré par une entreprise / un consortium
  - Projet open source géré par une entreprise ou un consortium
  - L'entreprise / les consortiums gèrent le processus de décision et les règles de gouvernance
- Géré par une fondation
  - Similaire à l'entreprise soutenue MAIS gérée par une fondation dédiée

- **PROTECTION INDUSTRIELLE**
  - Quel cadre pour quel besoin
  - Droit d'auteur
  - Logiciel libre et open source
- **PROTECTION DES USAGES: FOCUS SUR LES DONNÉES PERSONNELLES**
  - Evolution du contexte et des besoins
  - Loi informatique et libertés
  - Directive européenne et Safe Habour
  - RGPD et Privacy Shield
- **LÉGISLATION ET SOUVERAINETÉ NUMÉRIQUE**
- **POUR CONCLURE…**

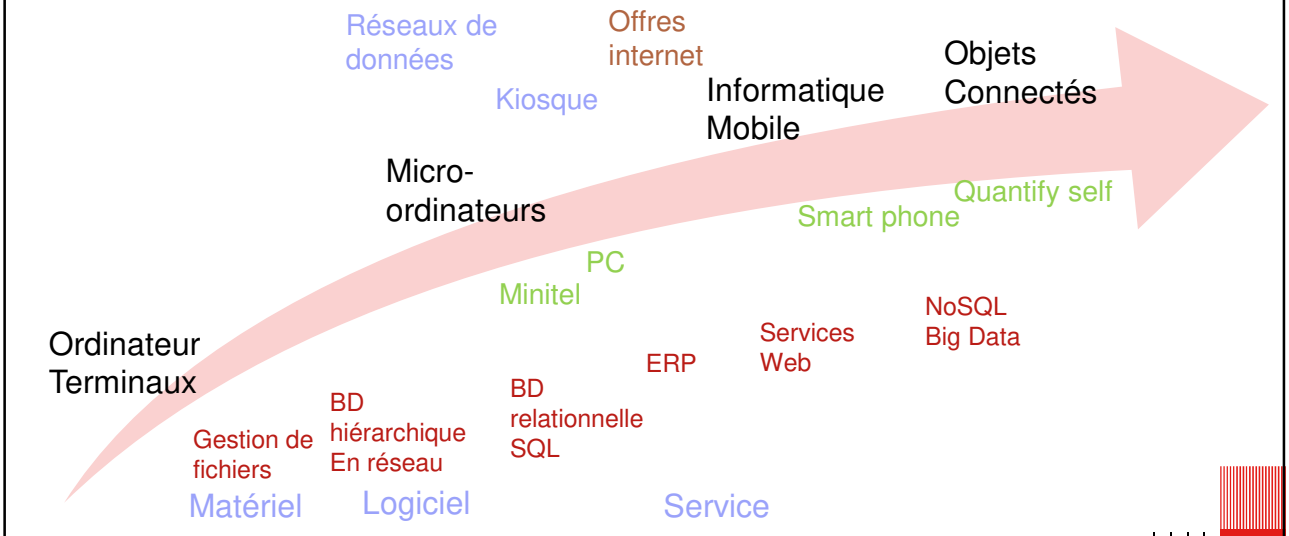
QUEL CONTEXTE POUR L'INFORMATIQUE?



DATA PRIVACY

- Données personnelles
  - Informations relatives à l'utilisateur
    - Nom, adresse, compétences, n° téléphone…
    - Adresse IP, nom machine, URL visitées...
  - Information relatives à l'activité
    - Log files, fichier journal des systèmes de contrôle d'accès
    - Contrôle « physique »
- Violation de la vie privée
  - Collecte de données personnelles
    - L'utilisateur doit en être informé
    - Données personnelles (privées) sur les machines
  - Analyse des données collectées

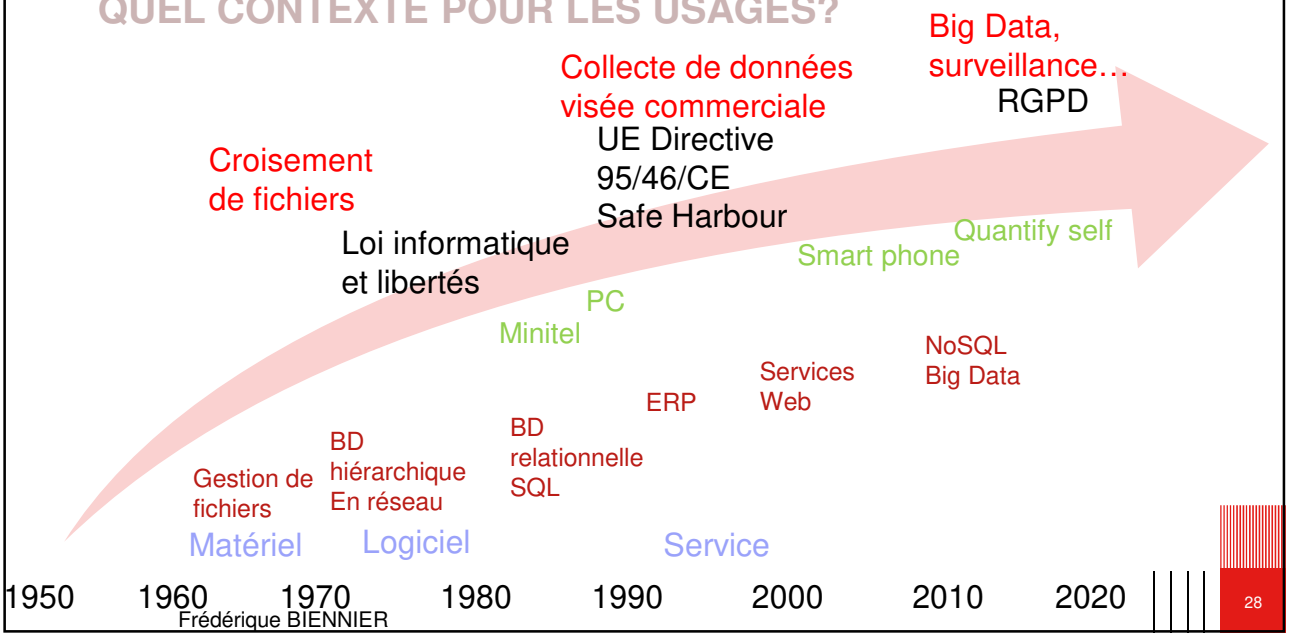
QUEL CONTEXTE POUR LES USAGES?



DE NOUVEAUX RISQUES ET DE NOUVEAUX MODÈLES

- Exploitation de données (personnelles) à grande échelle
  - Risque appréhendé dans les années 70
    - Développement des bases de données
    - « Croisement des fichiers »
    - « Identifiant unique » de l'INSEE
  - Une perception culturelle de ce risque
    - France et UE
      - Liée aux déportations / camps de concentration
    - US
      - Culture de la régulation par le marché
  - Evolution de la cible de la protection
    - Jumeau numérique?
    - Hausse des risques cyber

QUEL CONTEXTE POUR LES USAGES?



1978: LOI INFORMATIQUE ET LIBERTÉS

- 6 janvier 1978…
  - Avènement de Transpac
  - De plus en plus d'interconnexions entre SI
    - Numéro INSEE!
- Une loi française
  - Appelée à se développer dans un cadre de coopération internationale
  - Informatique « au service des citoyens »
    - Respect
      - Des droits de l'homme
      - Libertés individuelles et publiques
        - Religieuses
        - Syndicales
        - Politiques
    - Définition du droit à la vie privée

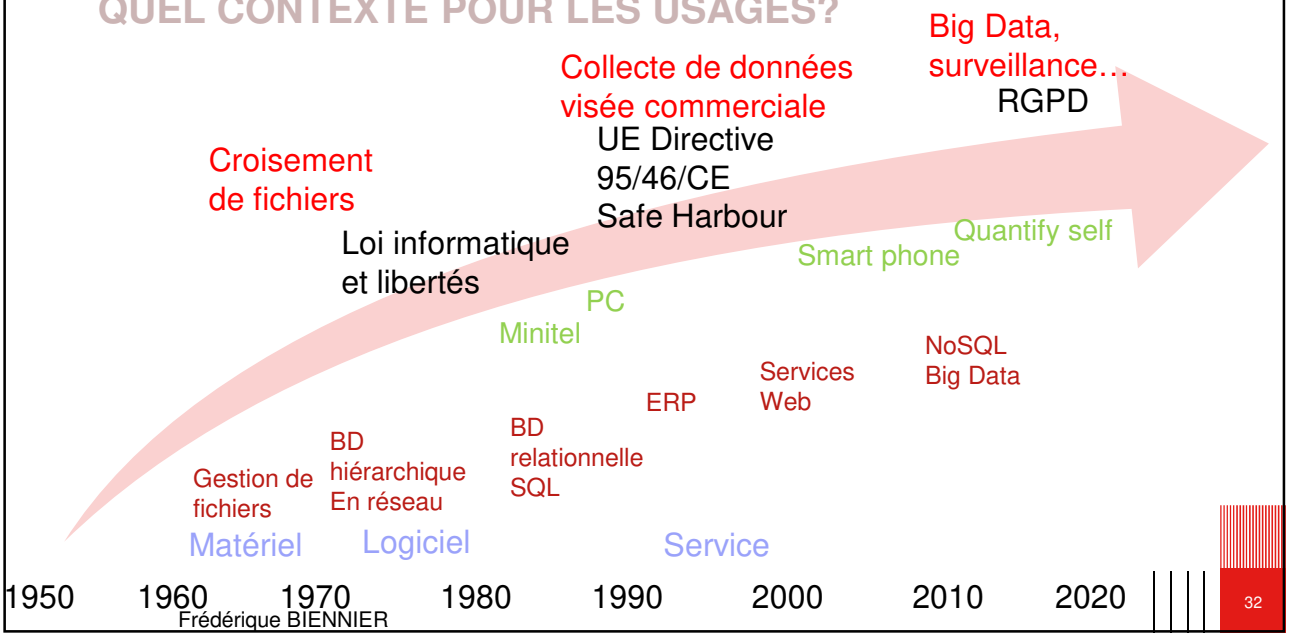
LOI INFORMATIQUE ET LIBERTÉS: DES DROITS ET DEVOIRS

- Cible
  - Identifier les informations utilisées
  - Connaître les motivations et périmètres des traitement
- Les devoirs des « ficheurs »
  - Déclarer les traitements
  - Usage proportionné et légitime des données
- Les devoirs des fichés
  - Apporter une information fiable
- Droits pour les fichés
  - Accès à leurs informations
  - Droit de rectification

LOI INFORMATIQUE ET LIBERTÉ: LE CONTRÔLE

- CNIL
  - Créée par la loi informatique et libertés
    - Commission de 18 membres nommés ou élus (présidence des assemblées, conseil d'état, cour de cassation, cour des comptes, conseil des ministres CESE, parlementaires, …)
    - Personnels dédiés
  - Organisation indépendante
    - Expertise techniques
    - Expertise juridiques
  - Déclaration et autorisation des fichiers
    - Formulaire type
  - Activité de contrôle
    - Fichiers informatique
    - Fichiers papier
  - Avis sur les différents projets de loi

QUEL CONTEXTE POUR LES USAGES?



BIG BROTHER IS WATCHING YOU…. PROTECTION DE LA VIE PRIVÉE

- Différents contextes légaux
  - Régulation par le marché : US
    - Federal Trade Commission
    - Les sites « abusifs » ne seront pas visités
    - Hyper-protection des mineurs de moins de 13 ans (accord parental certifié)
  - Cadre légal :
    - Privacy Act 1974
      - Citoyens américains
      - En lien avec le 5eme amendement (ni double incrimination ni auto-incrimination)
      - Protection concernant les fichiers fédéraux
    - UE Directive 95/46/CE
      - World wide protection pour les ressortissants de l'UE
      - Activités professionnelles et concernant la vie privée
- Enjeux majeurs
  - Echanges World wide
  - Cadre légal?
  - Principes communs
    - Fair et unfair practices
    - Safe harbour label pour vérifier les contraintes de l'UE

VIE PRIVÉE ET INTERNET… -

Traces / données laissées sur Internet
- Nom et adresse machine
- Paramètres machine
- Cookies
- Pages visitées

Collecte d'informations
- Identité
- Adresse mail
- Questionnaires divers
- En contrepartie
  - Bien
  - Service

Des pratiques pas toujours claires
- Vente de « fichiers clients »
  - Interdit au niveau EU selon la constitution du fichier
  - Pbs liés à l'exportation
    - Safe Harbour
- Avertissement sur la collecte de données
  - Ex Microsoft
- Traitement croisés sur les données collectées
  - Traces et reconstitution de workflow
  - Construction de profils de consommation
- Sécurisation des informations collectées

PRATIQUES JUSTES ET INJUSTES…

Pratiques « justes »

- Transparence
  - Collecte des données
  - Traitement des données
- Nécessité
  - Cyber-control utilisé conjointement avec d 'autres outils de sécurisation
- Equité
  - Objectifs du traitement des données personnelles
- Proportionalité
  - Cyber-control vs risques

Pratiques injustes

- Collecte de données…
- Durée de conservation des données collectées
- Processus croisés
- Vente des données personnelles

Conséquences

- Information des utilisateurs
- Déclaration légale
- Securisation du stockage et des processus de traitement des données personnelles
- Processus d 'analyse de ces données adapté
  - Eviter les processus d 'analyse croisée

Frédérique BIENNIER

35

LES PRINCIPES DE LA DIRECTIVE 95/46/CE

- Reprise de la loi Informatique et Libertés
- Vie privée
  - Travail
  - Personnelle
- 3 principes de base
  - Proportionnalité
  - Transparence
  - Légitimité du traitement
- Impose
  - Droit d'accès
  - Droit de rectification
  - Consentement

Frédérique BIENNIER

36

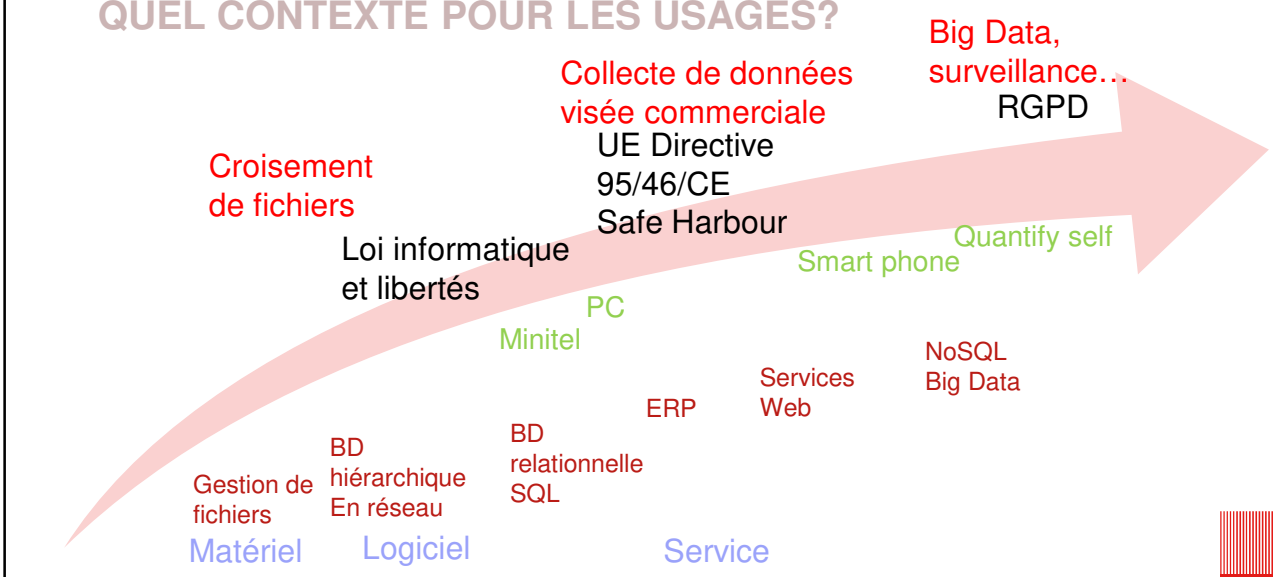
DATA PRIVACY AU TRAVAIL

- Espace personnel
  - Fichiers privés
  - Protection de la correspondance appliquée aux emails
  - Identification des utilisateurs
    - Login/password
    - Protection par clef physique associée à une PKI
- Contrôle relatifs à l'activité
  - Fichiers de reporting
    - Survivable systems
    - Usage des ressources, mesures de productivité...
  - Activity reporting
    - Re-construction des processus de Workflow
    - Risque de pistage du travail effectif

DIRECTIVE 95/46/CE VS SAFE HABOUR

- Directive 95/46/CE
  - Contrôle des pratiques justes
  - Concerne les citoyens européens
- Internet
  - Extra-territorialité
  - Différents environnements juridiques
- Safe Harbour
  - Respect des principes « justes »
  - Certification de sites
  - Pas de contrôles effectifs mais une information pour une régulation par le marché

QUEL CONTEXTE POUR LES USAGES?



Frédérique BIENNIER

39

SÉCURITÉ ET PROTECTION DES DONNÉES: NOUVEL AXE DE VALEUR?

- Marché de la donnée vs Ethique
  - La data permet de créer de la valeur
    - Vision commerciale
      - Directe => prospection et publicité
      - Indirecte => développement de nouveaux produits
    - Cœur de business
      - Traitements à valeur ajoutée
      - Gestion de la différenciation
  - Données personnelles
    - Risques juridiques pour les personnes
    - Risques de ciblage / discrimination
- De la sécurité des données à la protection de la vie privée
  - Evolution suit le développement de la vie numérique
  - Mettre de l'éthique dans le marketing: RGPD?

Frédérique BIENNIER

40

RGPD: C'EST QUOI?

- Règlement Général sur la Protection des Données (ou GRDP) : Règlement 2016/679 de l'UE
  - Les dates: publication le 27/4/2016 et mise en application au 25/5/2018
  - Les objectifs
    - Actualisation de la directive 95/46/CE
    - Extension de la notion de données personnelles
      - « Double numérique »
      - Accroissement des traces liant monde virtuel et monde réel
    - Cadre extra-territorial pour la protection des données
      - Prise en compte du développement de l'économie numérique
        - Big Data et profilage possible
        - Utilisateurs responsables (???)
      - Prise en compte des risques cyber
        - Impose la protection des données collectées
        - Droit à être prévenu en cas d'accès non autorisé / attaque
      - Principes repris du Safe Harbor
  - Un cadre juridique repris par différents pays: Canada, Argentine,…

RGPD: QUELLES DONNÉES SONT CONCERNÉES

- Les données personnelles classiques
  - Identification
  - Image
  - Génétique
  - Santé
  - Banque et finance
- Les données de la vie numérique
  - Traces
  - Consommation
  - Localisation
  - …
- Toutes les données relatives à une personne et permettant son profilage…

RGPD: QUELS TRAITEMENTS SONT CONCERNÉS

- Tous
  - Automatisés ou manuels
  - SAUF ceux réalisés par un individu à titre personnel
- Traitements classiques
  - En lien avec un SI et des processus bien identifiés
- Traitements statistiques
  - A vocation marketing
  - Intérêt de l'état
  - Lutte contre l'évasion fiscale
  - Sécurité des systèmes
  - Big Data et profilage SAUF ceux à visée discriminatoire
    - Caractères raciaux
    - Opinions (politiques ou religieuses)
    - Activités syndicales
    - …

RGPD: LES OBLIGATIONS DES ACTEURS ÉCONOMIQUES

- Obtention d'un consentement éclairé
  - Information donnée à l'utilisateur
    - Compréhensible?
    - Lue ?
  - Impact immédiat du double opt-in pour le mail
    - L'utilisateur ne doit pas seulement cocher une case mais donner confirmation
- Sécurité des données
  - Evaluation des risques et mise en place d'une politique de sécurité
  - Communication des vols de données aux intéressés dans les 72h
- Désignation d'un responsable sécurité des données (DPO)

RGPD: LES DROITS DES ACTEURS ÉCONOMIQUES

- Droits accrus
  - Possibilité de transfert transnationaux
    - Contrebalancée par l'extra-territorialité
  - Définition d'une chaîne de co-responsabilité avec les sous-traitants
    - Droit ou obligation?
  - Echanges marchands licites notamment pour la prospection (publicités ciblées en particulier!)
  - Traitements statistiques (lire Big Data) licites
    - Si non discriminatoires
    - Même sans consentement des personnes si ils répondent à un intérêt essentiel
      - Vie de la personne et santé publique
      - Intérêt de l'état et lutte contre l'évasion fiscale
      - Sécurité des systèmes

RGPD: LES DROITS DES UTILISATEURS

- « Personnes physiques vivantes »
  - Information nécessaire pour donner un consentement éclairé
  - Accès à l'ensemble des données personnelles (celles données explicitement et celles collectées automatiquement)
  - Droit à l'effacement (temps raisonnable) et droit à l'oubli
  - Droit de recours simplifié
    - Une seule autorité
    - Répercute la demande sur l'ensemble de la chaîne
  - Droit de récupérer les données de manière lisible et interopérable
  - Droit à la protection de leurs données
    - Etre averti en cas d'attaque

RGPD VS TRANSFERT DE DONNÉES AUX USA: PRIVACY SHIELD

- Safe Harbour dénoncé en 2015
  - Protection insuffisante dénoncée par la cour de justice
  - Pas de contrôle effectif
- Privacy Shield
  - Négocié en 2016
  - Intègre des contrôles
  - Possibilité pour un citoyen européen de saisir un médiateur en cas de violation
    - Permis par la Loi sur la réparation judiciaire (signe en février 2016)
    - Compte rendu publié
- MAIS
  - Accord dénoncé par la cours de justice européenne en 2020
    - Arrêt Schrems (Avocat autrichien)
    - Des atteintes disproportionnées à la vie privée
    - Des droits de recours limité
  - Impose de contrôle les flux !
- Négociation Privacy Shield V2 en cours

RGPD: MISE EN ŒUVRE (1)

- Quelques principes de mise en œuvre
  - Documentation des données et traitements
    - Analyse d'Impact de la Protection des Données (Data Protection Impact Analysis)
    - Analyse des processus (objectifs) et des données qu'ils manipulent
  - Nomination d'un DPO (souvent le Correspondant Informatique et Libertés!)
  - Privacy by (re)design
    - Intégration de la protection dès la conception
      - Analyse d'impact sur la vie privé (Privacy Impact Assessment)
    - Niveau d'exigence le plus élevé
  - Codes de conduite / labellisation
    - Apporter la preuve de la conformité
    - Intégration de la gestion des risques humains
  - Intégrer les aspects juridiques
    - Contrats
    - Recours

RGPD: MISE EN ŒUVRE (2)

- Qui est concerné par la mise en œuvre
  - La gouvernance d'entreprise
    - Direction
    - DPO / CIL
  - La DSI
  - Les directions métier (RH, marketing, ecommerce…)
- Comment évaluer la mise en œuvre
  - Questionnement spécifiques / acteur
    - Prise en compte des traitements
    - Prise en compte des objectifs
    - Prise en compte des processus de sécurisation
    - Cadre juridique
  - Lien important avec le niveau d'hygiène informatique

EXEMPLE DE CHECK LISTS SUR LA CONFORMITÉ (1)

- Gouvernance: l'organisation de la mise en conformité
  - DPO : nomination, indépendance
  - Maîtrise du périmètre d'application
    - Identification des Business Unit impactées, présence d'un registre de déclaration des traitements, inventaire des processus métier traitant des données personnelles, contrôle de conformité des sous-traitants, identification de transferts de données hors UE
  - Mise en conformité
    - Lancement d'un projet, contrôle de la feuille de route, reporting régulier, intégration de lma conformité dans les activités d'audit

EXEMPLE DE CHECK LISTS SUR LA CONFORMITÉ (2)

- Gouvernance: la gestion de la RGPD
  - Politiques et procédures
    - Durée de conservation, sécurité des données, suppression, notification si violation…
  - Veille juridique : La RGPD peut évoluer!
  - Assurance:
    - Intégration des risques liés aux données personnelles dans la couverture de l'entreprise
  - Formation
    - Diffusion des pratiques et intégration dans le programme de formation RH

EXEMPLE DE CHECK LISTS SUR LA CONFORMITÉ (3)

- Direction métier: les traitements et le contrôle d'accès
  - Licéité des traitement
    - Identification des finalités, de la proportionnalité, gestion du consentement, validation du croisement de données avec le DPO, gestion des durées de conservation
  - Types de traitement => consultation DPO
    - Profilage et traitements à haut risque (géolocalisation, contrôle d'accès aux locaux, vidéosurveillance…)
  - Types de données collectées (cf articles 9 et 10)
  - Droits des personnes
    - Information sur la collecte, demandes d'exercice de droits, modification du consentement

EXEMPLE DE CHECK LISTS SUR LA CONFORMITÉ (4)

- Direction métiers: la gestion des risques
  - Contractualisation avec des sous-traitants
  - Transfert de données hors UE et gestion des garanties associées
  - Sécurité des données personnelles
    - Définition des exigences auprès de la DSI, intégration des directions métiers dans les traitements / notifications de violation
  - Etude d'impact sur la vie privée (DPIA)
    - Identification de critères sur l'opportunité de l'étude d'impact, organisation de l'étude avec le DPO le cas échéant

EXEMPLE DE CHECK LISTS SUR LA CONFORMITÉ (5)

- Systèmes d'information et sécurité: la sécurité du SI
  - Cartographie du SI et des données personnelles
  - Sécurité des données personnelles
    - Intégration de la RGPD dans la politique de sécurité, intégration de bonnes pratiques et security by design, gestion des accès au système, sécurisation des accès administrateurs, mécanismes de protection (pseudonimisation et chiffrement)
  - Protection de la vie privée dès la conception
    - Moyens d'archivage et suppression, gestion de la rétention, isolation des environnements de production et de test

EXEMPLE DE CHECK LISTS SUR LA CONFORMITÉ (6)

- Système d'information et sécurité: Lien avec les contraintes juridiques
  - Contrôle des accès et usages
    - Traçabilité des accès sur les données, procédure de détection traitement et notification des violations
  - Relations aux sous-traitants
    - Intégration de la protection des données dans les contrats de sous-traitance, contrôle et audit régulier des sous-traitants
  - Etude d'impact
    - Définition de critères pour lancer un DPIA, méthode pour le DPIA
  - Processus permettant de répondre aux demandes d'accès (moins de 1 mois)

LES AVANCÉES ET LIMITES DE LA RGPD…

- La RGPD c'est
  - Un cadre juridique pour manipuler des données
  - L'introduction de l'extra-territorialité dans le monde d'Internet
  - Des droits et devoirs des fournisseurs de service
    - Contraintes pour prouver la bonne foi
  - Limité par les pratiques des utilisateurs eux-mêmes
    - Pas d'expérience sur l'extra-territorialité
    - Incohérence des échanges de données
    - Comment trouver « la root cause » de la divulgation d'une donnée personnelle
- Enjeu pour les fournisseurs de service
  - Comment prouver que la fuite ne vient pas d'eux
  - Comment identifier une intrusion rapidement : délai moyen de détection 240 jours!
- Repris par les législation de différents pays

- **PROTECTION INDUSTRIELLE**
- **PROTECTION DES USAGES: FOCUS SUR LES DONNÉES PERSONNELLES**
- **LÉGISLATION ET SOUVERAINETÉ NUMÉRIQUE**
  - Internet: un monde sans frontière?
  - Modèles pour la souveraineté
    - US
    - UE
  - Flux financiers et technologies Blockchain
- **POUR CONCLURE…**

LE CONTEXTE

- Internet
  - Objet technologique
    - Pile technologique
    - Partenaires bien identifiés
    - Pas de règlementation
      - Destiné à la recherche
  - De nouveaux moyens et usages
    - Réseaux sociaux
    - Recherche de contenu
    - Crypto-monnaies
    - …
  - Infrastructure
    - Communication
    - Centres de calcul
  - Des champions technologiques
- Quel(s) environnement(s) sur le plan légal?

SOUVERAINETÉ NUMÉRIQUE?

- Internet et le Web un monde ouvert?
  - Pas de notion de frontière
    - Majeure partie de l'infrastructure dans les eaux internationales?
    - Possibilité d'utiliser des VPN
  - Un partage universel?
    - Pas de contrôle / censure
    - Liberté totale?
- Un monde très contrôlé
  - Monde virtuel « connecté » au monde réel
  - Des impacts économiques et politiques
    - Contrôle via les entreprise offrant des accès ou des services
  - Notion d'extra-territorialité?

QUEL CADRE POUR LE MONDE NUMÉRIQUE COTÉ US?

- Statut des grands acteurs
  - Hébergeurs ou créateurs de contenus?
  - Section 230 du code des télécommunications
- Protection
  - De la vie privée: régulation par le marché
  - Des intérêts US
    - Patriot Act / Cloud Act / National Defense Authorization Act (Annuel…)
    - Règlementation au service de l'espionage industriel?
      - Discovery et e-discovery
        - Obligation du défenseur de fournir « toute information relative au litige »
        - Précision de la définition de l'objet du litige?

LE STATUT D'HÉBERGEUR: LA SECTION 230

- Diffusion d'Internet à grande échelle
  - Auto-régulation par le marché
    - Eviter les procès couteux!
  - Section 230 du code des télécommunications US
    - Liée à la liberté d'expression
    - Innovations et protection des « bébés champions »
    - Statut d'hébergeur
    - Evite les poursuites liées aux contenus tiers
      - Inclut les recommandations
  - Remise en cause du périmètre de la section 230 ?
    - Statut des recommandations
      - S'apparente à une production organisée de contenus / création d'une liste de lecture
    - Gonzales vs Google en cours à la cour suprême
      - Recommandation de contenus illicites
    - Questionne sur la modération
      - Censure ou modération?
      - Comment éviter les procès
        - Sur-modération
        - Sous-modération

PROTECTION DES INTÉRÊTS US…

- Patriot Act (2001)
  - Amende le Foreign Intelligence Surveillance Act (FISA) (1978)
    - Procédures de surveillance physique et électronique
    - Collecte et échange 'information sur les puissances étrangères
  - Impose aux FAI de fournir leur BB personnelles au FBI
- Clarifying Lawful Overseas Use of Data Act (Cloud Act) (2018)
  - Modifie le Stored Communications Act de 1986
  - Accès aux données personnelles (hébergées dans le Cloud)
  - Obligation aux fournisseurs de services établis sur le territoire US de fournir les informations sur tout citoyen ou résident US sur demande d'une instance judiciaire quel que soit son niveau
    - Fait abstraction du lieu de stockage des données
  - Contrevient au RGPD
  - Possibilité de l'utiliser pour de l'espionnage industriel
  - Peut être étendu avec des accords bilatéraux
    - A motivé la dénonciation du Privacy Shield
  - Semble opposé au 4eme amendement sur les saisies et perquisition faute de justification suffisante au mandat

PROTECTION DES INTÉRÊTS US ET ESPIONNAGE INDUSTRIEL

- Discovery
  - Le défenseur doit donner accès à toutes les informations concernant un litige
  - E-discovery
    - Implique de conserver tous les échanges électroniques (mails, documents…)
  - Périmètre large d'un contentieux
    - « Fishing expedition »
    - Atteinte au secret des affaires
- Protection?
  - French Blocking Statute : loi de 1968 mais les sanctions ne sont pas appliquées
  - Convention de la Haye (1970)
    - Impose de passer par la juridiction du pays signataire
    - De facto : mise en balance de l'intérêt des parties
  - Classement d'une information « secret des affaires
    - Directive de juin 2016 n° 2016/943
    - Harmonisation des procédures de blocage au niveau européen

QUEL CADRE POUR LE MONDE NUMÉRIQUE COTÉ UE

- Protection du secret des affaires
  - Directive de juin 2016 n° 2016/943
  - Harmonise le droit de blocage face au Discovery et e-discovery
- Maîtrise du marché et souveraineté
  - Organisation du marché de la donnée
    - Data act
    - Data governance Act
  - Numérique vu comme un moyen d'accéder au marché
    - Digital Market Act (2022)
- Protection des citoyens et de la société
  - Vie privée: RGPD (2016)
  - Interactions avec le monde numérique: Digital Service Act (2022)
  - Risque concernant le respect des droits fondamentaux : AI Act (en cours)
- Rôle de « précurseur » et diffusion des principes

LE MARCHÉ DE LA DONNÉE, UN ENJEU MAJEUR ?

- La donnée, un moteur de développement et d'innovation
  - Production en hausse croissante
  - « Carburant » pour les « nouveaux » développement
    - Data science
    - IA et apprentissage automatique
- Valeur d'une donnée
  - Dépend de l'usage
  - Liée à son coût
    - Acquisition
    - Stockage
    - Traitement

ESSAI DE CATÉGORISATION DES DONNÉES

Classification selon le contexte de génération

- Données transactionnelles
  - Issues du SI / site web propre
  - Niveau de confiance important
  - Propriété bien identifiée (?)
- Données analytiques
  - Dérivées des données transactionnelles (BI, Big Data analytics…)
  - Ajoute une valeur ajoutée propre
- Données Big Data
  - Donnée interne ou externe indépendante du SI classique
  - Générée par un utilisateur, un capteur…
- Classification en fonction du « secret »
  - First party => générées par le SI (?) / l'entreprise
  - Partagées = > Impliquent un partenaire commercial
  - Publiques => Open data

Classification en fonction de l'espoir de gain / valeur attribuée

- Junk data
  - Données publiques
  - En dehors du champs d'activité
- Données dilemme
  - Données à disposition (SI classique ou données de l'utilisateur via le site Web, réseaux sociaux…)
  - Pas encore de clé de valorisation
- Données concurrencées
  - Largement disponibles et utilisées par les concurrents
  - Peu différenciantes
  - Trouver une direction de valorisation
    - Enrichissement par confrontation avec les données de l'entreprise
    - Restitution offrant une VA
- Données stratégiques
  - Données rares, propriété de l'entreprise
  - Potentiel de valorisation connu

OPEN DATA VS MARCHÉ DES DONNÉES

- Open Data: mise à disposition (gratuite) de données
  - Bénéfice tiré par la proposition de nouveaux usages
  - Conserver une relative maîtrise sur ces usages
  - Rentabilité de la collecte?
    - Contrôle des usages pour éviter la concurrence
    - Rendre la collecte plus éthique?
    - Données pour la recherche
    - Données « urbaines »…
- Marché des données
  - Toute information a un prix
    - Fonction de l'usage qui en sera fait
    - Fonction du service apporté
      - Location (usage limité) vs achat (pas de limitation d'usage)
      - Pré-traitement
  - Des rôles divers
    - Courtage
    - Système de collecte
    - Stockage de Data Lake
- Question: qui est le propriétaire d'une donnée?

DATA GOVERNANCE ACT

- Pilier de la stratégie européenne des données
  - Permettre le développement de nouveaux services numérique
  - Conserver la maîtrise de la « valeur »
- Adopté par la commission en 2020
  - Voté en 2022
  - Mise en application en septembre 2023
  - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767
- Cible
  - Utilisation de données personnelles impliquant un acteur d'intermédiation
  - Mise à disposition de données du secteur publiques soumises au droit d'autrui
  - Partage de données (non personnelles) entre entreprises
  - Partage de données altruiste

CE QUE LE DGA INTRODUIT

- Cadre juridique concernant
  - La réutilisation de données
    - Exclusivité sauf cas d'intérêt général interdite
    - Auorisée dans le respect du droit à la propriété intellectuelle
    - Indication claire des conditions d'autorisation pour la réutilisation
  - La définition de service d'intermédiation
    - *un service qui vise à établir des relations commerciales à des fins de partage de données entre un nombre indéterminé de personnes concernées et de détenteurs de données, d'une part, et d'utilisateurs de données, d'autre part, par des moyens techniques, juridiques ou autres, y compris aux fins de l'exercice des droits des personnes concernées en ce qui concerne les données à caractère personnel*
    - Obligations pour les prestataires
      - Ne pas utiliser les données pour eux-mêmes
      - Mise en place de procédures pour prévenir les autorisations frauduleuses
      - Prévenir les « propriétaires » de données en cas de problème
  - Partage altruiste des données
    - Partage gratuit
    - Transparence de l'utilisation
    - Objectif d'intérêt général
- Certifications
  - Intermédiation
  - Usage altruiste

DATA ACT

- Proposition de la commission du 23/2/2022
  - Pas encore adoptée au parlement
  - Complète le DGA
  - Etend la protection des données personnelles aux autres types de données
- Objectif
  - Meilleure répartition de la valeur entre les acteurs de l'économie de la donnée (personnelle ou non)
  - Règles harmonisées relatives à l'accès et à l'utilisation équitables des données
    - Développement économique des activités liées à la donnée pour les acteurs de l'UE
    - Cadre juridique cohérent
  - Favoriser la disponibilité des données et leur utilisation
    - Permettre le partage des données IoT
    - Interopérabilité et portabilité des données
    - Favoriser le partage de données (B2B et B2C)
  - Réduire les abus et déséquilibres contractuels

TRANSFORMATION NUMÉRIQUE : DMA

- Digital Market Act (2022)
  - Déséquilibre entre plateformes et les entreprises qui les utilisent
  - Gatekeeper
    - Fournit des services essentiels: services d'intermédiation, moteurs de recherche, réseaux sociaux, navigateurs web, assistants virtuels, plateformes de partage de vidéos, messageries non fondées sur la numérotation, systèmes d'exploitation, services cloud, services de publicité dont les services d'intermédiation publicitaires.
    - Position permettant de bloquer l'accès au marché
      - « Zone de chalandise » numérique: utilisateurs / mois
      - Capitalisation importante
      - Les gatekeepers sont notifiés de ce statut
    - Identification de 24 obligations / interdictions
      - Liés aux collectes de données
      - Au droit de choisi des installations logicielles
      - A la non concurrence déloyale
      - Respect du RGPD
      - Articles 5, 6 et 7 du Chapitre III (https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022R1925&from=EN)
  - Contrôles et amendes dissuasives

Graphique 2 - Les effets concurrentiels attendus des obligations et interdictions du *DMA*

Obligations et interdictions du DMA	Concurrence plus saine au sein de la plateforme régulée*	Concurrence hors plateforme plus forte**	Plus forte contestabilité des positions du gatekeeper***
Éviter la concentration de données en imposant le consentement des utilisateurs: 5 (2)	++	++	+++
Interdiction des clauses de parité tarifaire: 5 (3)	+	+++	+++
Principe de liberté commerciale des utilisateurs professionnels: 5 (4)	+	+++	+++
Principe de liberté d'accès des utilisateurs finaux aux services de plateforme essentiels y compris lorsque cet accès a eu lieu de façon désintermédiée: 5 (5)	++	+++	+++
Interdiction de limiter la capacité des utilisateurs à signaler les pratiques des gatekeepers auprès de toute autorité publique compétente: 5 (6)	+	+	+
Interdiction d'offres liées: 5 (7, 8)		+	+++
Transparence de la chaîne d'intermédiation publicitaire: 5 (9, 10)	+++	+	+++
Interdiction d'utiliser les données des entreprises utilisatrices concurrentes du gatekeeper: 6 (2)	+++	++	+
Liberté d'abonnement, installation/ désinstallation d'applications et paramétrage (navigateur, moteur de recherche, assistant virtuel): 6 (3, 4, 6)	+++	+	+++
Interdiction d'auto-préférence du gatekeeper dans les classements, l'indexation et le crawling: 6 (5)	+++	+	+++
Interopérabilité des services accessoires et objets connectés: 6 (7)	++	++	+++
Accès gratuits aux métriques de performance publicitaire: 6 (8)	+++	++	
Portabilité des données des utilisateurs finaux: 6 (9)		+	+++
Accès aux utilisateurs professionnels des données qu'ils génèrent: 6 (10)	+++	++	+
Partage des données de recherche aux moteurs de recherche tiers: 6 (11)			+++
Conditions FRAND: 6 (12)	+++	+++	
Conditions générales de résiliation des services (par les utilisateurs) proportionnées: 6 (13)		+++	+++
Interopérabilité des fonctionnalités de base des messageries: 7			+++

- Source: https://www.entreprises.gouv.fr/files/files/en-pratique/etudes-et-statistiques/themas/thema-7-le-digital-markets-act-regulation-des-grandes-plateformes-numeriques.pdf

TRANSFORMATION NUMÉRIQUE: DSA

- Digital Service Act
  - A destination des utilisateurs
    - Donner un cadre plus sure à la vie numérique
  - Améliorer la transparence
    - Conditions générales à jour, claires, compréhensibles et non ambigües
    - Mécanismes de recours et réparation
    - Traitements internes dont modération
  - Respect du RGPD
  - Correspondant pour chacun des états membres
  - Amendes dissuasives
    - 6% du CA mondiale et astreinte de 5% du CA mondial

DSA: LES OBJECTIFS

- Souveraineté européenne
  - Favoriser le développement des PME et services numériques sur le marché européen
  - Préserver les droits fondamentaux
    - liberté d'expression et d'information
      - Lutte contre la diffusion de contenus illicites (au sens du droit) et la désinformation
    - principe de non-discrimination
    - respect du niveau élevé de protection des consommateurs
    - …
  - Protection individuelle
    - Interdiction de la publicité ciblée aux mineurs
    - Endiguer le cyber-harcèlement
  - Protection collective
    - Agir contre les contenus avec effets négatifs réels ou prévisibles sur
      - la sécurité publique
      - les processus démocratiques et électoraux

PROJET DE RÈGLEMENTATION UE SUR L'IA RESPONSABLE

- L'intelligence artificielle revêt une importance capitale pour notre avenir. Aujourd'hui, nous sommes parvenus à atteindre un équilibre délicat qui stimulera l'innovation et l'adoption de la technologie de l'intelligence artificielle dans toute l'Europe, avec tous les avantages que cela présente, d'une part, et dans le plein respect des droits fondamentaux de nos citoyens, d'autre part.
  - *Ivan Bartoš, vice-Premier ministre tchèque chargé de la transformation numérique et ministre du développement régional*
- Projet de la commission européenne datant d'avril 2021
  - Stratégie pour le marché unique numérique
    - Concurrence juste et équitable
    - Respect des principes de l'UE
  - Subsidiarité (UE vs état)
    - Principe de libre circulation
    - Marché unique numérique
  - Proportionnalité
    - Gestion des risques
    - Exigence de transparence

« AI ACT » DE L'UNION EUROPÉENNE

- Objectif
  - Permettre et contrôler le développement de l'IA
    - Enjeu économique
    - Contrôle de l'accès au marché européen
  - En respectant les libertés fondamentales
    - Protection des citoyens et de règles communes
- Pas d'éthique ou de moral dans la loi…
  - Basé sur la notion de risques
  - Centré sur l'impact sur les Hommes et la société
- Proposition de la commission
  - Cycle d'approbation

AI ACT: CHAMPS D'APPLICATION

- Protection des citoyens et des droits fondamentaux
  - Conditions sur le déploiement dans l'UE
  - Conditions sur l'impact sur des individus dans l'UE
- Cible
  - Organismes, fournisseurs, distributeurs et importateurs de systèmes d'IA
    - A destination d'individus de l'UE ou ayant un impact sur un individu de l'UE
    - D'un système déployé au sein de l'UE
  - Utilisateurs
    - Des systèmes d'IA
    - Des résultats produits par un système d'IA
- Dérogations
  - Usage privé et non commercial
  - « Autorisations spéciales » pour les états et organismes dans le cadre d'accords internationaux de coopération policière ou judiciaire avec l'UE ou l'un des pays membre

LES ENJEUX DE L'AI ACT…

Définir un système d'IA

- Dimension systémique et usage
- Par rapport à un logiciel « normal »
  - Apprentissage automatique
  - Règle de logique
  - Exploitation de connaissances
- Couverture large
  - Neutre technologiquement
  - Garantie la pérennité

IA sûre

- Préserver les droits fondamentaux
  - Egalité
  - Non-discrimination
  - Inclusion
  - Dignité humaine
  - Liberté
  - Démocratie
- Contrôle des usages et de leur contexte
  - Usage privé
  - Usage commerciale
  - Sureté de l'état

AI ACT: LE CADRE PROPOSÉ

Usage selon

1) Cible du système
   - Rôle du composant
   - Domaine d'application
2) niveau de risque
   - Inacceptable => Interdit
     - Rares dérogations
   - Très élevés => Exigences
     - Qualité
     - Contrôle, divulgation, suivi
     - Supervision humaine
     - Gestion
       - Logs
       - Sécurité, précision et robustesse
       - Gouvernance des données
       - Documentation; tests…
   - Limité => Transparence

Le cadre proposé

- Niveau UE
  - Commission
  - Groupe d'experts
  - AI Board
- Niveau de chaque état
  - Notifying authority
    - Avis
    - Processus de désignation, évaluation, notification des organismes de contrôle
  - Autorité de surveillance nationale
    - Point de contact
    - Membre du AI Board
  - Market surveillance authority
    - Surveillance activités du marché
    - Communication avec autorité de surveillance nationale
- Organismes de certification et contrôle

AI ACT: UNE CLASSIFICATION DES RISQUES (1)

- Risque inacceptable = Usage de l'IA interdit (Article 5)
  - Manipulation du comportement, des décisions subliminale pouvant conduire à un dommage sur l'intégrité physique ou psychologique
  - Exploitation de personnes vulnérables, de personnes handicapées mentales ou d'enfants entraintant un préjudice physique ou psychologique
  - Reconnaissance biométrique à distance et en temps réel dans l'espace public pour le maintien de l'ordre (sauf autorisation spéciale)
  - Classification sociale des individus

AI ACT: UNE CLASSIFICATION DES RISQUES (2)

- Risque très élevé = Usage soumis à contrôle (article 6)
  - Finalité
    - Composant orienté sécurité
    - Systèmes d'IA autonomes
      - Point d'attention sur la conformité avec la règlementation existante
      - Certaines décisions ultimes reviennent à l'Homme
  - Domaine d'application (Annexe 3 mise à jour annuellement)
    - Identification biométrique et catégorisation de personnes physiques
    - Gestion et exploitation d'infrastructures critiques
    - Éducation et formation professionnelle
    - Emploi, gestion des collaborateurs et accès au travail indépendant
    - Accès et jouissance aux services privés essentiels et aux services et prestations publics
    - Application du droit
    - Gestion de migrations, d'asile et de contrôles aux frontières
    - Administration de la justice et processus démocratiques

AI ACT: UNE CLASSIFICATION DES RISQUES (3)

- Risques limités = soumis à une obligation de transparence
  - Systèmes agissant en interaciton avec des humains
  - Systèmes à base de données biométriques
    - Détection d'émotion
    - Catégorisation (sociale)
  - Génération ou manipulation de contenus
    - Trucages ultra réalistes
    - Vidéo, images, textes…

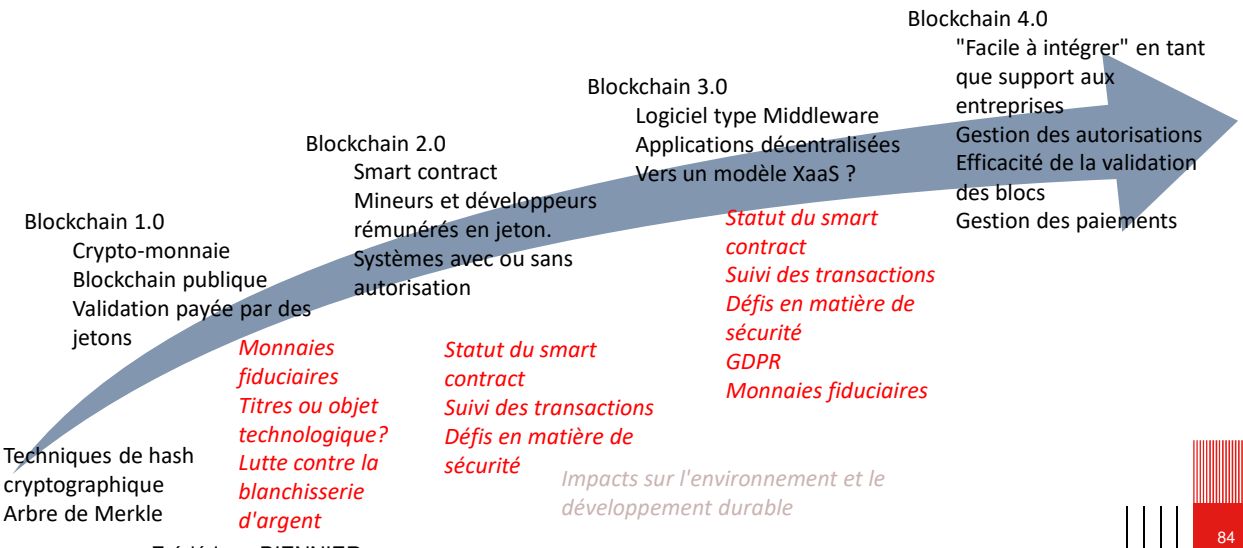
ET POUR CE QUI CONCERNE LES FLUX FINANCIERS?

- Transaction financière
  - Monnaie fiduciaire
    - Privilège régalien
    - Adossée à une garantie
  - Gestion de transaction
    - Propriétés ACID
    - Traçables
      - Travel Information
      - Identification précise de l'émetteur et du receveur
    - Des législations différentes selon les pays
      - Optimisation fiscale
      - Mise en place de structures complexe pour le blanchiment
- Sur Internet
  - Pas de gestion de transaction en natif
    - Blockchain
    - Crypto-actifs: une monnaie dédiée à Internet?
  - Interroge sur la souveraineté

Frédérique BIENNIER

83

DÉFIS LIÉS À LA RÉGLEMENTATION DE LA BLOCKCHAIN



Frédérique BIENNIER

84

STATUT JURIDIQUE DE LA BLOCKCHAIN

- France : 2015 - Loi « Macron 2 » modernisation de l'économie
  - Le gouvernement français peut autoriser les « distributed ledgers » pour l'émission et l'enregistrement des mini-obligations (mini-bond)
  - Les transactions associées peuvent être reconnues comme des contrats juridiques
  - Extension aux instruments financiers enregistrés
  - Mise en place d'un cadre juridique
- États-Unis : mars 2017
  - Chambre de l'Arizona
  - a "distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is theoretically immutable and auditable and provides an uncensored truth"

SMART CONTRACT

- Transaction automatisée ou contrat au sens légal ?
  - Mise en œuvre d'un "contrat du monde réel«
  - Processus limité
- Conclure un contrat implique
  - Parties identifiées
    - Comment relier la "véritable identité" à la pseudo-identité de la Blockchain ?
    - Une erreur d'identification sur une partie peut entraîner (ou non) la nullité du contrat
  - Les parties disposent de la capacité à contracter
    - Comment prouver que la partie pseudo-identifiée a bien la capacité de contracter ?
    - Par exemple, seules les personnes majeures peuvent signer un contrat. Qu'en est-il des mineurs ?
- Code is law vs Code of law
  - De la réglementation technique à la réglementation juridique
  - Utilisation et contexte

JETONS ET CRYPTO-ACTIFS

- Statut du jeton
  - Valeur d'usage
    - Nécessaire à l'exécution d'une tâche / à l'utilisation du système
    - Les frais de transaction sont un « droit de péage »
  - Valeur financière
    - Moyen de paiement
    - Placement => Titre (Security)
- Test de Howey (US) pour identifier les titres
  - Investissement en argent dans une entreprise "commune
  - Bénéfice attendu
  - Pas de possibilité de changer la gouvernance de l'entreprise
- Des règlementations différentes
  - Impact sur l'émission des jetons (ICO / STO)
    - Initial Coin Offer => Participation à la gouvernance
    - Security Token Offer => Soumis aux autorités de régulation des marchés financiers

PRINCIPES CLÉS DE LA RÉGLEMENTATION DES ACTIFS VIRTUELS

- Initial Coin Offer
  - Pour le projet blockchain
    - Levée de fonds
    - Moins réglementé que le marché financier ?
  - Pour les investisseurs
    - Investissements en titres
    - Être intégré dans la gouvernance du projet
  - Pour les régulateurs
    - Titres
    - Autorités de régulation spécifiques selon les pays
    - Prévention de la fraude
- Transactions
  - Traces
  - Identification du donneur d'ordre et du bénéficiaire

Source : https://fr.cryptonews.com/guides/the-difference-between-ico-and-sto.htm

MOTIVATION POUR UN CADRE JURIDIQUE

- Souveraineté
  - Gestion des monnaies fiduciaires
    - Les crypto-actifs pourraient être interdits (Chine, Egypte...)
  - Fiscal
- Risques
  - Investisseurs
  - "Impact sur l'économie réelle
  - Systèmes de financement du crime et du terrorisme
- Recommandation mondiale
  - Groupe d'action financière (GAFI / FATF Financial Action Task Force)
  - Lutte contre la blanchisserie d'argent

EXIGENCES RÈGLEMENTAIRES POUR LES FINTECH

	Crypto-actifs	Technologie de grand livre distribué	Systèmes de paiement
Modification du périmètre réglementaire	X		X
Informations aux consommateurs	X		X
Limites à l'accès des investisseurs de détail	X		
Gouvernance des entreprises			X
Gestion des risques par les entreprises		X	X
Résilience opérationnelle des entreprises		X	X
Protection des données		X	X
Lutte contre le blanchiment d'argent	X		
Concentration et concurrence		X	X

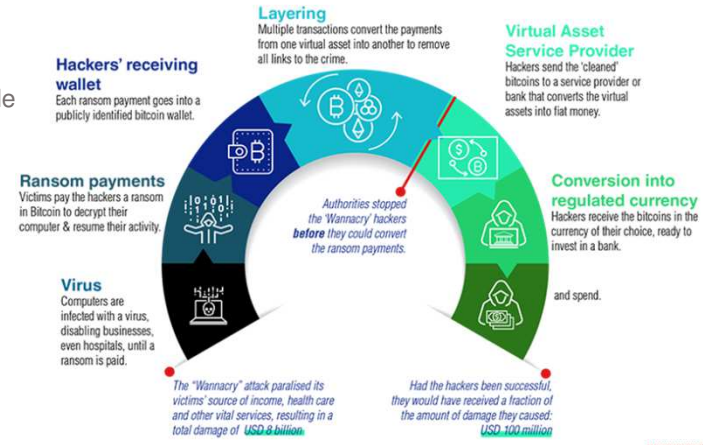
Source : https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/03/regulation-and-supervision-of-fintech.pdf

MARCHÉ EUROPÉEN DES CRYPTO-ACTIFS (MICA)

- Conçu pour faire face aux risques liés aux crypto-actifs
  - Protection des consommateurs
  - Souveraineté monétaire
  - Exclure NFT
- Fournisseurs de services de crypto-actifs
  - Autorisation d'exercer dans l'UE
  - Protection des portefeuilles des consommateurs
  - Responsabilité en cas de perte des crypto-actifs des investisseurs
- Déclaration d'empreinte environnementale
- StableCoin
  - Pas de spéculation
  - Réserve de liquidité
  - Retrait gratuite à tout moment
- MiCA:
  - Adoption par le conseil en juin 2022 et octobre 2022 ar le parlement pour un déploiement en 2024
  - https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52020PC0593

EXIGENCES EN MATIÈRE DE BLANCHIMENT

- Cycle de vie du blanchiment
  - « Coins » à l'échelle internationale
  - Pas de gestion de l'identité
  - Monnaies indépendantes
  - Acteurs multiples
- Impact réel sur l'économie
  - Motive la régulation
  - Moyen de limiter le hacking



Source : https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)

LES EXIGENCES DU TOFR

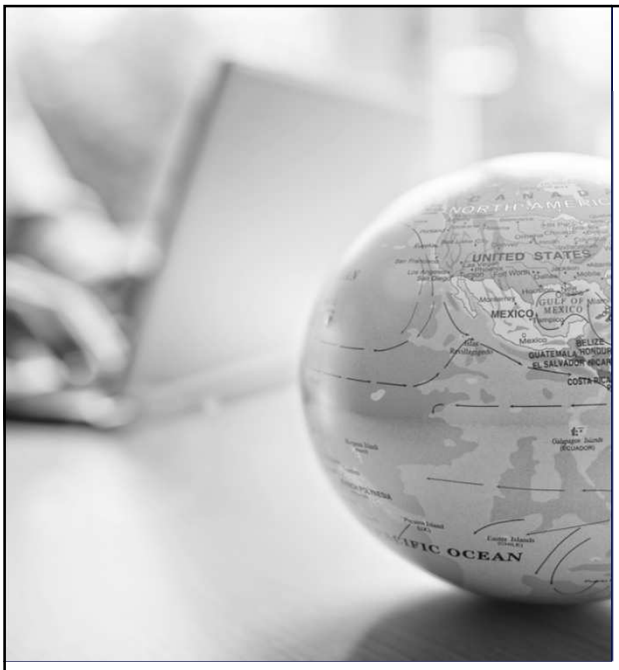
- Transfert of Fund Regulation
  - Portée internationale
  - Pas de seuil d'application
  - Crypto-asset = flux financier classique
    - Intégration des « travel information » pour intégrer la traçabilité
    - Obligation pour les Vitrtual Asset Service Provider (VASP)
- Identité réelle
  - Identité prouvée
  - Identités de l'émetteur et du bénéficiaire recueillies et stockées par le VASP chargé d'exécuter le transfert.
  - Impacte également les portefeuilles non hébergés (c'est-à-dire les portefeuilles qui ne sont pas conservés par un tiers)
- Champ d'application international
  - Toute entreprise fournissant des services de biens virtuels dans l'UE
  - Mesures de conformité renforcées pour toute interaction entre les VASP de l'UE et ceux des pays tiers
  - Inclusion de l'ensemble de la chaîne de VASP intermédiaires => Transmission du donneur d'ordre initial et du bénéficiaire tout au long de la chaîne
- Régulation opérée par
  - Autorité européenne des marchés financiers (AEMF)
  - Autorité bancaire européenne (ABE)
  - Tenue d'un registre des VASP non conformes
- Protection des données
  - RGPD
  - Conditions d'application définies par le Comité européen de protection des données

RÈGLEMENT DE L'UE SUR LE TRANSFERT DE FONDS

- Actif virtuel
  - Similaire aux services financiers traditionnels
  - Transactions sous pseudonyme
- Les « Travel rules » financières
  - Identités avérées
  - Informations sur la source et le bénéficiaire associées à la transaction
  - Stockage sécurisé de la transaction de part et d'autre
- Stopper les flux illicites dans l'UE
  - Transférer les « Travel rules » aux crypto-actifs
  - Responsabilité du fournisseur de services de crypto-actifs
    - Enregistrer la transaction
    - Vérifier la fiabilité de la source
- Adoption par le parlement européen en octobre 2022 pour une application en 2024

POINTS CLEFS DE LA RÈGLEMENTATION US

- Évolution de la réglementation
  - Actifs numériques, y compris NFT
  - De la régulation du marché libre à l'intégration de la loi sur le secret bancaire
  - Faire face aux atteintes à la stabilité financière et à la sécurité nationale
- Des défis similaires à ceux du GAFI
  - Développement responsable des biens virtuels
  - Contrôle des transferts de fonds
  - Réglementation des valeurs mobilières



- **PROTECTION INDUSTRIELLE**
- **PROTECTION DES USAGES: FOCUS SUR LES DONNÉES PERSONNELLES**
- **LÉGISLATION ET SOUVERAINETÉ NUMÉRIQUE**
- **POUR CONCLURE…**

POUR CONCLURE…

- D'une technologie à un monde numérique
  - Législation construite de manière incrémentale
    - Protection industrielle
    - Protection des personnes
    - Organisation financière
  - Ouverture ?
    - Bien commun
    - Interaction avec le monde réel

TRANSFORMATION NUMÉRIQUE ET RÈGLEMENTATION

- **« La transformation numérique est une nécessité. Pas un « bon à savoir », pas un « beau à avoir », mais un impératif si vous voulez rester dans la course et gagner contre les criminels. »**
  - T. Raja Kumar, président du GAFI (2022-2024) lors de la conférence du GAFI sur la numérisation, juin 2022.
- Un univers virtuel en prise avec l'univers réel
  - Transposition de règles et lois pour définir un « vivre ensemble »
  - Complexité liée à l'internationalisation
    - Propagation contraignant l'ouverture de marchés
    - Extraterritorialité
  - Des enjeux
    - De souveraineté
    - De protection des biens et des personnes
  - Des questions éthiques
    - Place de l'IA
    - Protection de la vie privée

CADRE LÉGISLATIF ET RÈGLEMENTATION

- Construction du cadre européen
  - Basé sur la protection des droits fondamentaux
    - Valeurs de l'UE reconnues par tous les membres
    - Protection de la vie privée
  - Maîtrise de la souveraineté européenne
    - Régulation des services et du marché du numérique
    - Contrôle d'accès au marché européen
      - Certifications de conformité
      - Instances de contrôle
      - Pénalités financières lourdes
    - Possibilité de Sandbox pour permettre l'émergence de champions européens
- Vers un statut « légal » pour la transformation numérique?
  - Effet d'entrainement à l'échelle mondiale
  - Encore de nombreuses exceptions!