



- LE DROIT DES
- DONNÉES
- PERSONNELLES

ISAE SUPAERO

Programme du cours

Aujourd'hui (mardi 7 janvier)

Matin

- Introduction au droit à la vie privée (1h)
- Présentation du RGPD (2h)

Après-midi

- Initiation aux autres textes en droit du numérique (1h30)
- Présentation des modalités d'évaluation (15min)
- Cas d'étude : Google Spain (1h15)

Le mois prochain (mercredi 5 février)

Évaluation : procès fictifs

Enjeux démocratiques

Politique / Société

Cambridge Analytica, l'incarnation de la triche électorale rendue possible par Facebook

April Glaser — Traduit par Jean-Clément Nau — 21 mars 2018 à 8h58 — mis à jour le 21 mars 2018 à 9h14

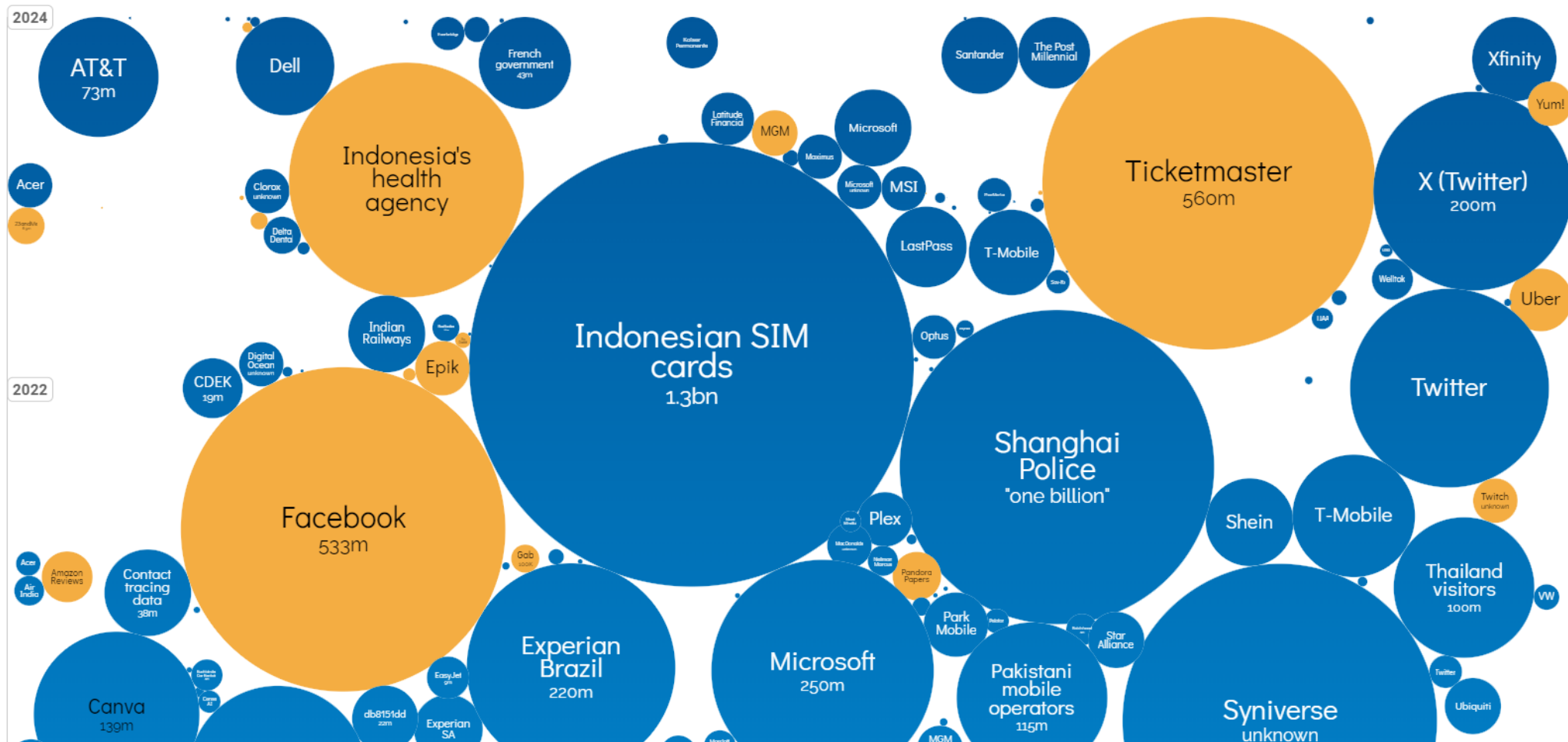
Pendant la campagne électorale de 2016, la campagne de Donald Trump aurait fait main basse sur les données de cinquante millions d'utilisateurs.

Scandale Cambridge Analytica -
Facebook



Brexit

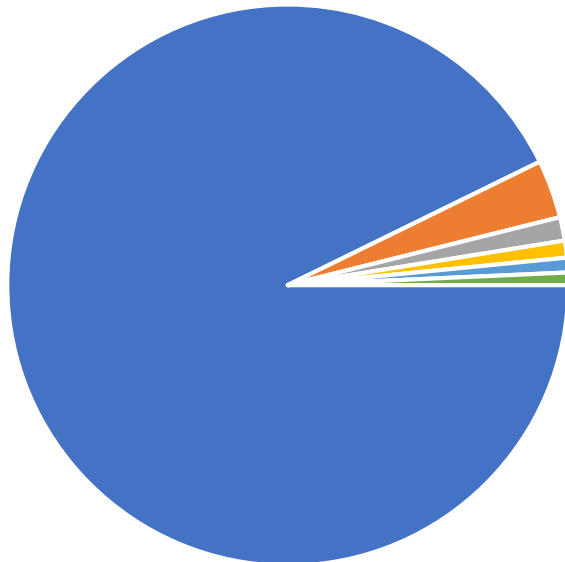
Enjeux de sécurité des données





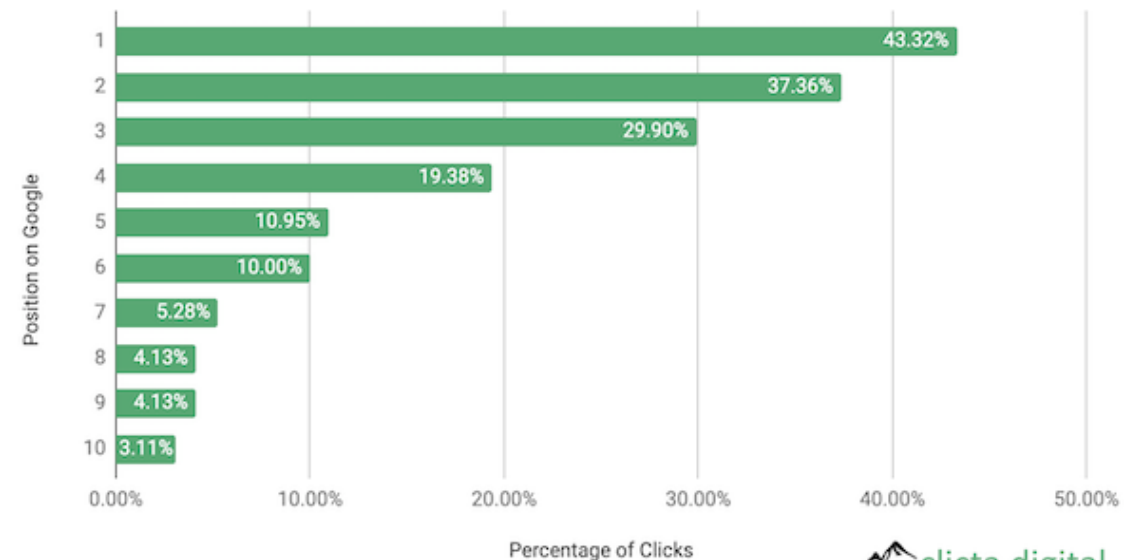
Enjeux concurrentiels

Marché mondial de la recherche internet
(Aout 2022)



■ Google ■ Bing ■ Yahoo! ■ Yandex ■ Baidu ■ Duckduckgo

Average Google Click-Through Rate by Position



clicta digital

Importance du référencement Google (2020)


Enjeux économiques

Bruxelles inflige une amende record de 4,34 milliards d'euros à Android


Pour la commissaire européenne Margrethe Vestager, Google se sert de son système d'exploitation « pour consolider la position dominante » de son moteur de recherche.

Amazon écope d'une amende record de 746 millions d'euros au Luxembourg

Le régulateur luxembourgeois a infligé une amende d'un montant inédit au géant américain pour non-respect de la protection des données. Le géant américain, qui juge la décision « sans fondement », devrait faire appel.

 Lire plus tard

 Commenter

 Partager

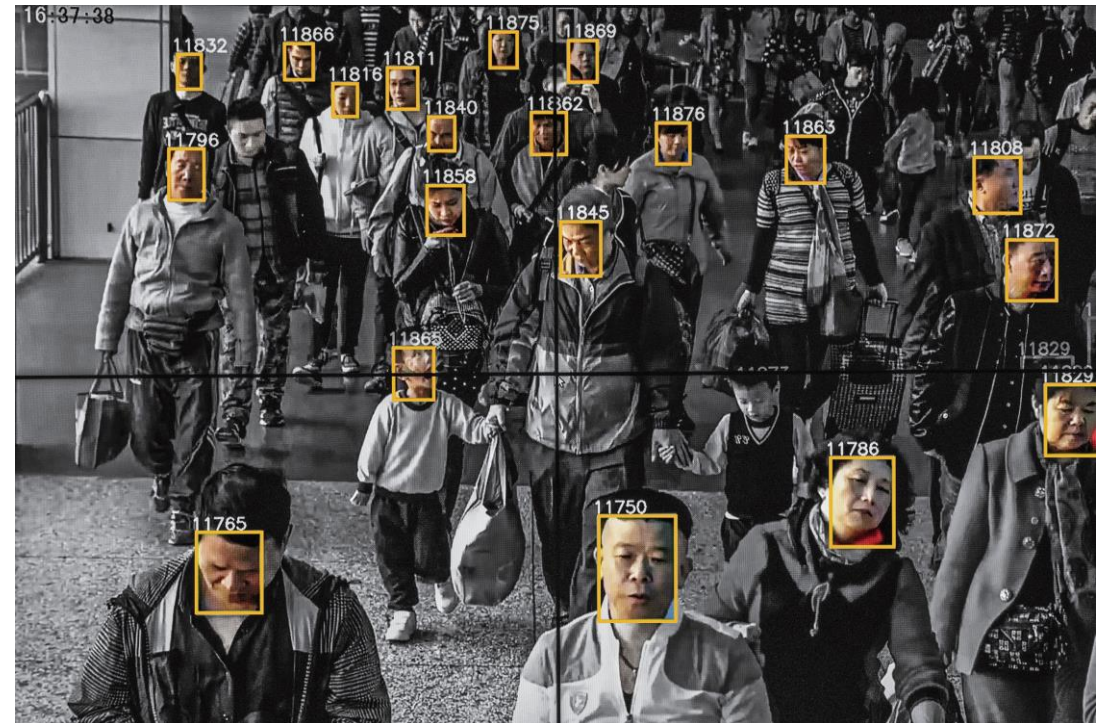
 Amazon

 Confidentialité des données

Enjeux de sécurité



Vidéosurveillance



Score de crédit social en Chine


La vidéosurveillance en France

Reconnaissance faciale dans les lycées : la Cnil dit non

Technologie : "Ce dispositif concernant des élèves, pour la plupart mineurs n'apparaît ni nécessaire, ni proportionné" explique la Commission. Reste que cette technologie est en pleine croissance en France.

Reconnaissance faciale : le tribunal de Marseille vire les portiques virtuels de deux lycées

Dans ta face

26 • 16 

Le droit à la vie privée

Un droit fondamental, protégé par les textes internationaux, européens et nationaux :

- Article 12 de la Déclaration Universelle des Droits de l'Homme des Nations Unies ([lien](#))
- Article 8 de la Convention Européenne des Droits de l'Homme ([lien](#))
- Article 9 du Code Civil ([lien](#))

→ Englobe le droit à la protection des données à caractère personnel, protégé par :

- Article 8 de la Charte des Droits Fondamentaux de l'Union Européenne ([lien](#))



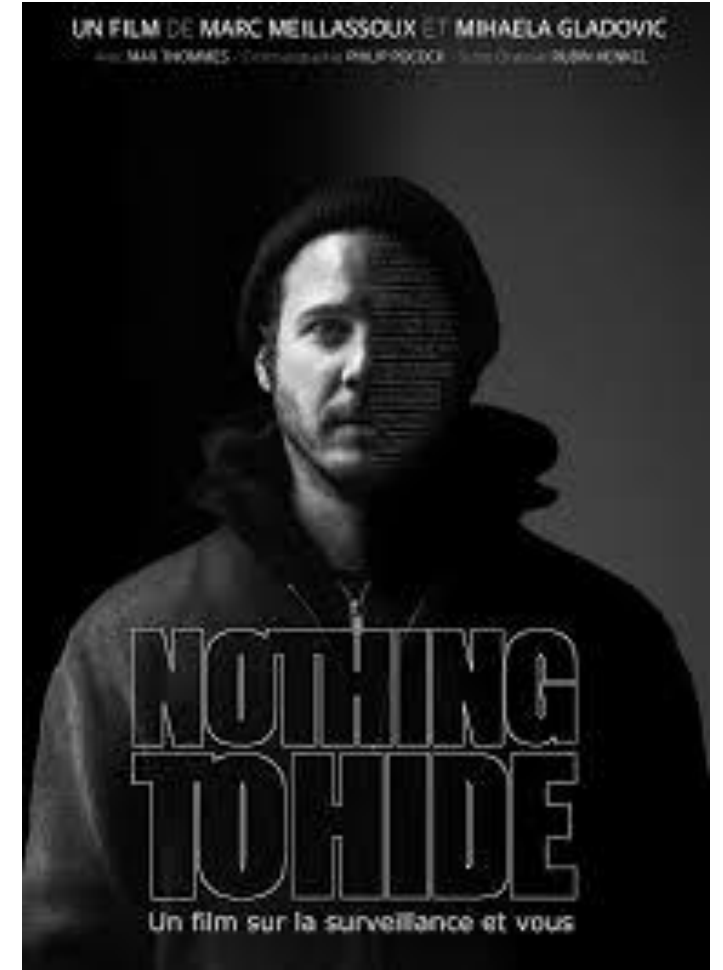
La notion de vie privée



Capitalisme de surveillance,
Shoshanna Zuboff



*« Arguing that you don't care
about the right to privacy because
you have nothing to hide is no
different than saying you don't
care about free speech because
you have nothing to say »*
- Edward Snowden



Nothing to hide ([bande-annonce](#))

PARTIE 1 : INTRODUCTION SUR LA RÉGLEMENTATION DES DONNÉES PERSONNELLES

Le Règlement Général à la Protection des Données personnelles (RGPD)



- Voté en 2016 et entré en vigueur le 25 Mai 2018
- Remplace une directive européenne de 1995
- Application large
- Logique de mise en conformité
- Sanctions très importantes en cas de violation

La notion de traitement de données

Définition : « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel »

Exemples : 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 ou l'interconnexion, la limitation, l'effacement ou la destruction



- Toute action en rapport avec des données personnelles est un traitement !
- Toutes les entités réalisent des traitements !

Qu'est-ce qu'une donnée personnelle ?



Nom / Prénom



Photos satellites



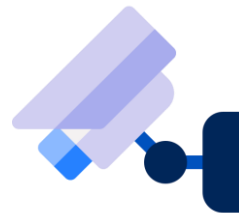
Numéro de
téléphone d'une
entreprise



Adresse email
professionnelle



Régime alimentaire
d'un client



Enregistrement
vidéosurveillance

Une adresse IPv4 (notation décimale à point)

172 . 16 . 254 . 1

Adresse IP

Les types de données à caractère personnel

Données personnelles

Définition : « *Toute information se rapportant à une personne physique identifiée ou identifiable* »

Identification directe : nom/ prénom ; numéro de sécurité sociale ; empreinte digitale ...

Identification indirecte : plaque d'immatriculation, numéro de téléphone, adresse IP ...



La personne identifiée ou identifiable est appelée la « personne concernée »

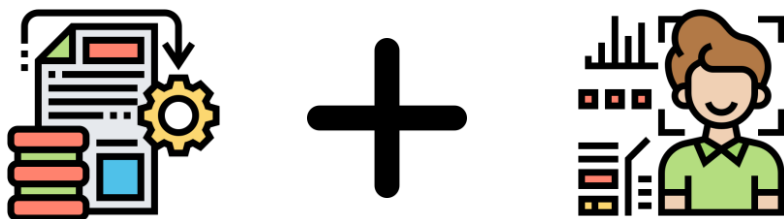
Données personnelles «sensibles»

Données révélant :

- Origine raciale ou ethnique ;
- Opinion politique ;
- Convictions religieuses ou philosophiques ;
- Appartenance syndicale ;
- Données génétiques ou biométriques ;
- Santé ;
- Vie sexuelle ou orientation sexuelle ;

Champ d'application

Champ d'application matériel



Présence d'un traitement de données à caractère personnel

Champ d'application territorial



Le responsable de traitement ou le sous-traitant se situe sur le territoire de l'EEE

OU

Les personnes concernées se trouvent sur le territoire de l'EEE

Les différents acteurs 1/2



Responsable(s)
de traitement

- **Choisit les finalités et les modalités** du traitement
- **Responsabilité** civile et pénale en cas de manquement



Sous-traitant

- Traite les données **pour le compte du responsable** de traitement
- Doit **respecter les directives** du responsable de traitement ET les règles sur les données personnelles



Responsabilité solidaire entre le responsable de traitement et le sous-traitant pour la personne concernée

Les différents acteurs 2/2



Délégué à la Protection des Données personnelles (DPD)

Qui est-ce ?

- Personne avec des compétences sur le droit à la protection des données et/ou informatique ;
- Interne ou externe à l'entreprise ;

Que fait-il ?

- Veille à la conformité des traitements de l'entreprise ;
- Point de contact des personnes concernées et de la CNIL ;
- Conseille le responsable de traitement, le sous-traitant mais aussi leurs employés ;



Autorité de régulation française : la CNIL

- **Informe** les acteurs de leurs obligations ;
- **Conseille** les acteurs sur la façon de remplir leurs obligations ;
- **Reçoit les plaintes** des individus en rapport avec la réglementation des données personnelles ;
- **Contrôle** les acteurs qui traitent des données personnelles
- **Sanctionne** en cas de non-conformité

PARTIE 2 :

LES OBLIGATIONS DU RESPONSABLE DE TRAITEMENT ET DU SOUS-TRAITANT



Finalités du traitement

- 1 Les finalités doivent être déterminées, explicites et légitimes.
- 2 Les données doivent être traitées exclusivement pour atteindre la/les finalité(s) choisies !

Conséquences : Toutes vos actions sur les données doivent être proportionnelles avec les finalités



- Pas de recours à des moyens disproportionnés !
- On ne récolte pas de données si elles ne sont pas nécessaires
- Pas de réutilisation des données personnelles !

Licéité du traitement

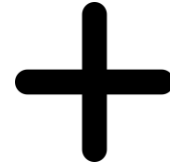
Le RGPD pose une liste de 6 justifications possibles pour rendre un traitement licite :

- 1 Le **consentement** de la personne concernée
- 2 **Exécution d'un contrat** avec le responsable de traitement
- 3 Respect d'une **obligation légale**
- 4 Sauvegarde **des intérêts vitaux** d'une personne physique
- 5 Réalisation d'une **mission d'intérêt public**
- 6 Nécessaires à la réalisation des **intérêts légitimes**

Exigences sur les données



Données exactes



Données tenues à jour



- Possibilité de corriger ses données
- Effectuer la modification dans les différentes bases contenant la donnée en question
- Répercuter ce changement sur les décisions prises sur le fondement de cette donnée
- Vérifier régulièrement l'exactitude des données en cas de changement de contexte



Supprimer rapidement des données erronées ou obsolètes !



La durée de conservation

1 Définir la durée

Conservation **proportionnelle**
à la finalité du traitement

Exemples de durée maximum:

- Pour les cookies = **13 mois**
- Pour les vidéos de surveillance = **1 mois**

2 Après la fin du délai

- Suppression des données, ou
- Conservation dans un but de recherche ou de statistiques, ou
- Anonymisation des données.

Transfert de données hors de l'UE

RAPPEL

Si les données proviennent d'europpéen ou sont traitées en UE,
la réglementation (RGPD) s'applique à ces données



Toutes ces données doivent bénéficier
d'un niveau de protection uniforme !



Protection équivalente obligatoire pour tous les
acteurs impliqués dans le traitement de données,
même s'ils sont situés hors de l'UE

Transfert de données hors de l'UE

Conséquences pratiques



- Lister les individus ayant un droit d'accès aux données.
- Conserver pour chaque destinataire / utilisateur de données le type de donnée auxquels il a accès / qu'il a reçu.



- Identifier les pays où les données sont situées et transférées.
- Identifier les pays où résident ceux ayant accès aux données.



- Communiquer ces informations au service juridique et collaborer avec lui si besoin.



Si les données sont transmises à des personnes non conformes à la réglementation, votre entreprise est sanctionnable !

Transfert de données hors de l'UE

La notion de décision d'adéquation

Une décision de la Commission européenne établissant qu'un pays tiers, par l'intermédiaire de sa législation interne ou de ses engagements internationaux, offre un niveau de protection des données à caractère personnel comparable appliqué dans l'Union européenne.

L'exemple des États-Unis



Sécurité et Violation de données

DÉFINITION : destruction, perte, altération, divulgation non autorisée ou accès non autorisé, de manière accidentelle ou intentionnelle, de données à caractère personnel.

1 Avant la faille de sécurité

- Mise en place des mesures organisationnelles et techniques proportionnées :



- Chiffrement
- Mot de passe sécurisé
- Eviter le BYOD
- Back up régulier ...

2 Après la faille de sécurité

- Signaler et expliquer le contexte et les conséquences potentielles de la faille :



- Décrire les données concernées
- Lister les personnes concernées
- Et répondre à tout autre question interne



Sanctions possibles

- Rappel à l'ordre
- Injonction de mise en conformité (astreinte possible)
- Suspendre ou arrêter le traitement
- Impact sur l'image de l'entreprise
- Amende administrative
- Sanctions pénales



Montant maximum de l'amende :
20M € ou 4% du CA mondial

Exemples d'amendes administratives



Sécurité des données des clients insuffisante

→ 400.000 €



Manquement à la sécurité +
Durée de conservation

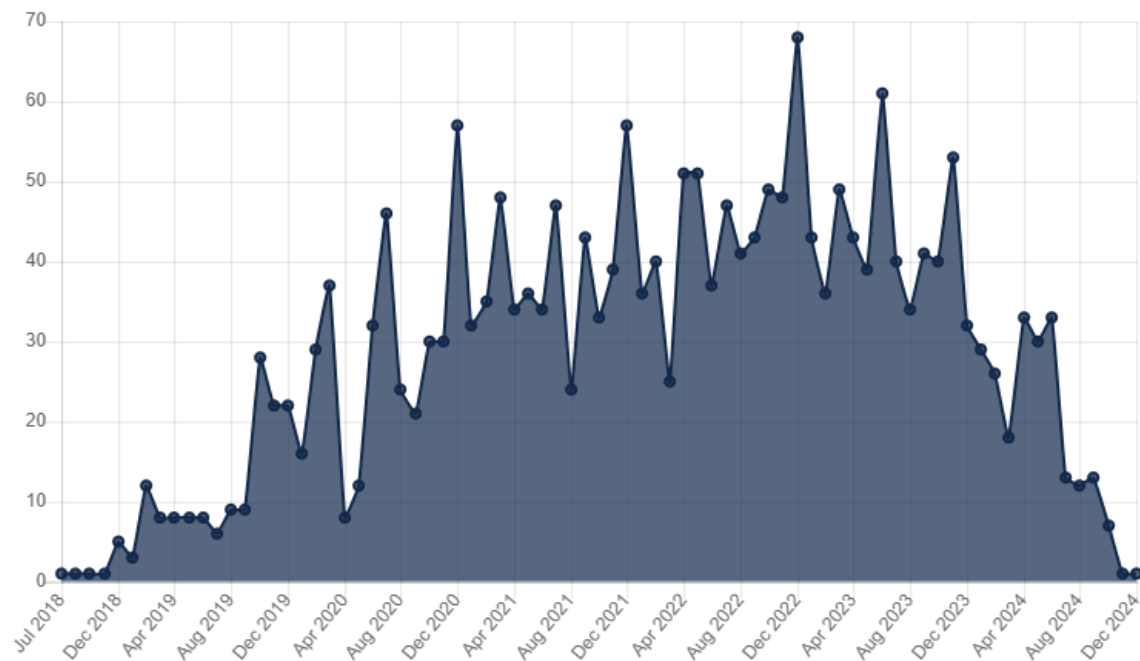
→ 400.000 €



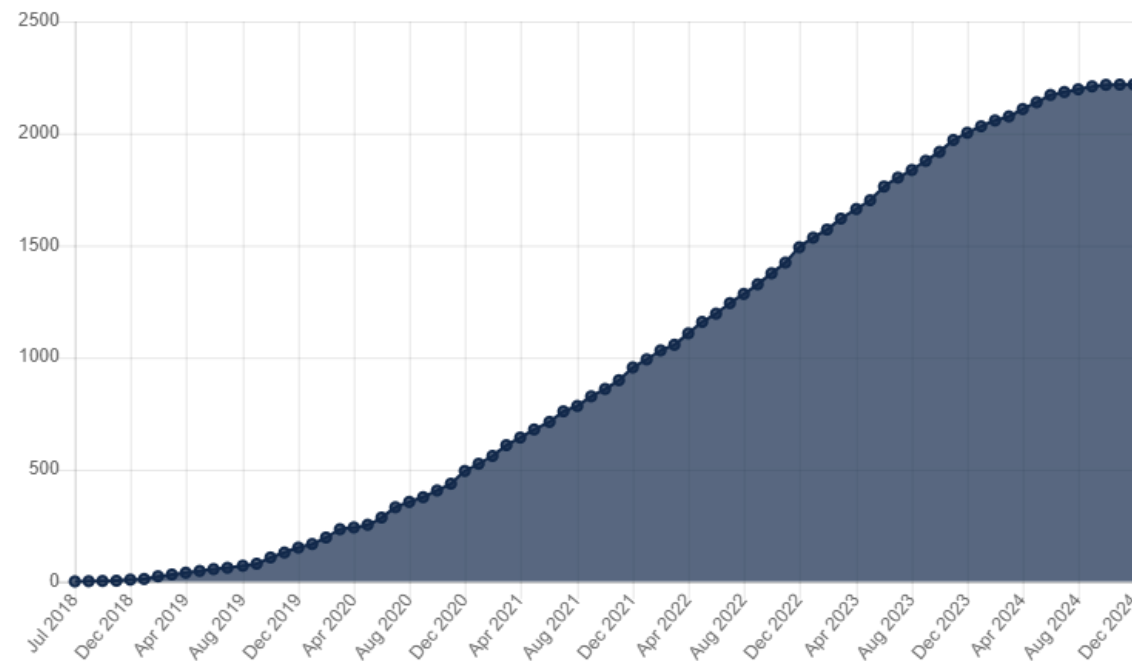
Manque de transparence +
Obligation d'information + Absence
de consentement pour la publicité

→ 50.000.000 €

Évolution des sanctions dans le temps

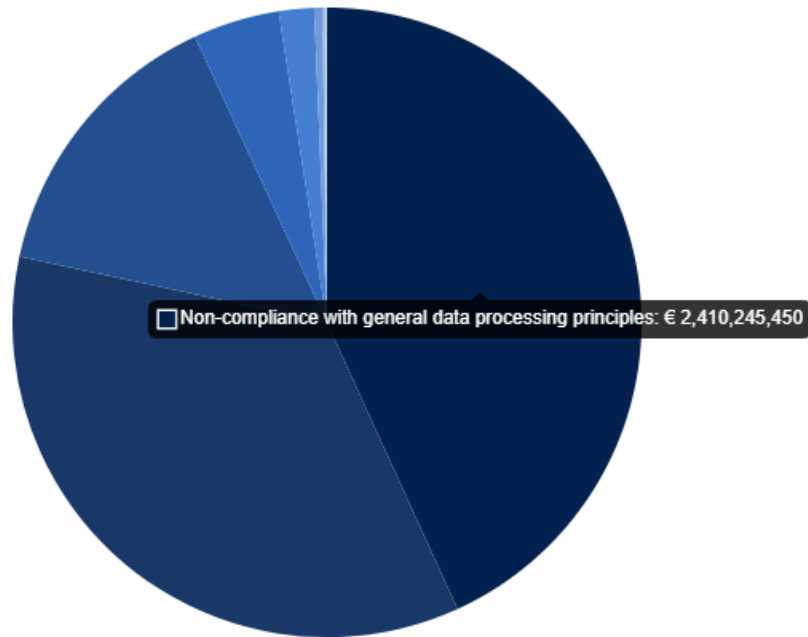


Nombre d'amendes par mois



Nombre d'amendes en cumulé

Causes de sanctions



Violation	Sum of Fines
Non-compliance with general data processing principles	€ 782,638,364 (at 176 fines)
Insufficient fulfilment of information obligations	€ 234,946,895 (at 61 fines)
Insufficient legal basis for data processing	€ 182,992,138 (at 298 fines)
Insufficient technical and organisational measures to ensure information security	€ 68,583,119 (at 176 fines)
Insufficient fulfilment of data subjects rights	€ 16,316,825 (at 78 fines)
Unknown	€ 14,700,500 (at 4 fines)
Insufficient fulfilment of data breach notification obligations	€ 1,284,091 (at 20 fines)
Insufficient data processing agreement	€ 993,580 (at 5 fines)
Lack of appointment of data protection officer	€ 229,000 (at 8 fines)
Insufficient cooperation with supervisory authority	€ 213,929 (at 34 fines)

PARTIE 3 :

LES DROITS DES PERSONNES CONCERNÉES

Droit à l'information



Dans les textes :

Informations à communiquer à la personne concernée :

- Identité du responsable de traitement ;
- Finalités du traitement ;
- Base légale ;
- Destinataires de vos données ;
- Durée de conservation ;
- Droits de la personne concernée ;
- ...

Art. 12 RGPD



Dans la pratique :

ARTICLE 1 : Objet

Les présentes « conditions générales d'utilisation » ont pour objet l'encadrement juridique des modalités de mise à disposition des services du site [Nom du site] et leur utilisation par « l'utilisateur ».

Les conditions générales d'utilisation doivent être acceptées par tout Utilisateur souhaitant accéder au site. Elles constituent le contrat entre le site et l'Utilisateur. L'accès au site par l'Utilisateur signifie son acceptation des présentes conditions générales d'utilisation.

Éventuellement :

- En cas de non-acceptation des conditions générales d'utilisation stipulées dans le présent contrat, l'Utilisateur se doit de renoncer à l'accès des services proposés par le site.
- [Nom du site] se réserve le droit de modifier unilatéralement et à tout moment le contenu des présentes conditions générales d'utilisation.

ARTICLE 2 : Mentions légales

L'édition du site [Nom du site] est assurée par la Société [Nom de la société] [SAS / SA / SARL, etc.] au capital de [montant en euros] € dont le siège social est situé au [adresse du siège social].

[Le Directeur / La Directrice] de la publication est [Madame / Monsieur] [Nom & Prénom].

Éventuellement :

- [Nom de la société] est une société du groupe [Nom de la société] [SAS / SA / SARL, etc.] au capital de [montant en euros] € dont le siège social est situé au [adresse du siège social].

L'hébergeur du site [Nom du site] est la Société [Nom de la société] [SAS / SA / SARL, etc.] au capital de [montant en euros] € dont le siège social est situé au [adresse du siège social].

ARTICLE 3 : Définitions



J'ai lu et j'accepte les conditions

Droit d'accès aux données personnelles



Dans les textes :

Informations à communiquer sur demande :

- Les informations vues précédemment
- Les données que possède le responsable de traitement ;
- La « logique sous-jacente » de l'algorithme utilisé le cas échéant ;
-



Dans la pratique :





Google Dashboards





Paramètres > Vos données twitter



Raccourcis de confidentialité

	Droit à la rectification	Droit à la limitation	Droit d'opposition
Définition et Objectif 	<ul style="list-style-type: none"> • Corriger les données inexactes • Compléter les données existantes 	<ul style="list-style-type: none"> • « Geler » l'utilisation de vos données • Empêcher toute action sur vos données attente de l'exercice d'un de vos droits 	<ul style="list-style-type: none"> • S'opposer à l'utilisation de nos données pour un traitement précis • Justifier par « des raisons tenant à votre situation particulière »
Acteurs concernés 	Le responsable de traitement + Le sous-traitant		

	Droit à la portabilité	Droit à l'effacement
Définition et Objectif 	<ul style="list-style-type: none"> Récupérer les données que vous avez fournies à la plateforme Transférer ces données d'une plateforme à l'autre <p><u>Remarque</u> : Les données sont dans un format lisible par la machine.</p>	<ul style="list-style-type: none"> Effacer ou déréférencer des données personnelles vous concernant <p><u>Exemples</u> : photos ou liens gênants</p> <p><u>Remarque</u> : ce droit ne s'applique que dans certaines situations. Pensez à vous renseigner avant de faire la demande</p>
Acteurs concernés 	Le responsable de traitement	Le responsable de traitement + Les sous-traitants

Droit à la notification des failles de sécurité



Dans les textes :

Si la faille de sécurité peut entraîner un risque élevé pour les droits et libertés de la personne concernée, alors il l'informe :

- De l'existence de la faille ;
- Des données concernées ;
- Des conséquences possibles ;
- Des mesures prises et à prendre pour limiter les répercussions.



Dans la pratique :



OU



« Nous avons fait l'objet d'une faille de sécurité concernant vos données personnelles. Ce n'est pas très grave mais veuillez changer votre mot de passe svp »

Des questions ?



INTRODUCTION AU DROIT DU NUMÉRIQUE

PARTIE 1 :

LE DROIT DES PLATEFORMES EN LIGNE

Les opérateurs de plateformes en ligne

Professionnel proposant un service de communication en ligne reposant sur :

1

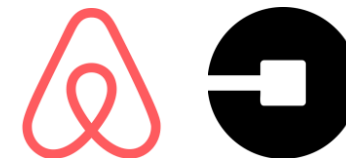
Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers



OU

2

La mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service





L'information au consommateur

Information claire, loyale et transparente présente dans une rubrique spécifique :

- 1 Conditions de référencement et de déréférencement des contenus
- 2 Les critères de classement par défaut des contenus ainsi que leurs principaux paramètres
- 3 Existence d'une rémunération ou lien capitalistique qui influencerait le classement ou le référencement



Le cas des *fake news*

Définition : « *allégations ou imputations inexactes ou trompeuses d'un fait de nature à altérer la sincérité du scrutin à venir sont diffusées de manière délibérée, artificielle ou automatisée et massive* »



Sanctionnable par le juge sur saisine (l'auteur de la news + la plateforme)



Dans une période de 3 mois avant une élection générale



Limité aux informations ayant un impact sur l'élection



Le droit des plateformes en ligne : le règlement *Digital Services Act* (DSA)



Objectif

Encadrement des plateformes en ligne afin de protéger les utilisateurs contre les contenus illicites présents



Entrée en vigueur

1

Acteurs nommés depuis 2022

2

Entièrement applicable depuis février 2024



Sanctions

1

6% du CA annuel mondial pour manquement aux obligations

2

1% CA mondial annuel pour informations trompeuses et manque de collaboration



Le droit des plateformes en ligne : le *Digital Services Act* (DSA)



Obligation de publication d'un rapport de transparence annuel :

Sur le recours à des « moyens automatisés »

- 1 Objectifs précis confiés aux outils utilisés
- 2 Indicateurs utilisés pour mesurer la précision des outils
- 3 Mesures de sauvegardes appliquées, si existantes



Le droit des plateformes en ligne : le *Digital Services Act* (DSA)



Obligation de transparence pour la publicité en ligne :

- 1 Existence d'une publicité affichée
- 2 Éléments d'identification du commanditaire de la publicité
- 3 Paramètres utilisés pour déterminer la cible de la publicité



Le droit des plateformes en ligne : le *Digital Services Act* (DSA)



Interdictions concernant les systèmes de recommandation :

- 1 Interdiction de proposer des pubs ciblées en fonction d'un profil basé sur des données sensibles pour les adultes
- 2 Interdiction de publicité ciblée pour les mineurs
- 3 Pour les très grandes plateformes, obligation de proposer un système de recommandation non fondé sur le profilage



DSA : le cas des « très grandes plateformes » et des « très grands moteurs de recherche »

Critères de qualification

1

Nombre d'utilisateurs
moyen $\geq 45\text{M}$ / mois

+

2

Désignation par la
Commission européenne

Exemples des entreprises concernées



Très grandes plateformes (20)



Très grands moteurs
de recherche (2)



DSA : le cas des « très grandes plateformes »



**Obligation d'évaluation
des risques systémiques**

- 1** Diffusion de contenus illicites
- 2** Effets négatifs sur les droits fondamentaux
- 3** Manipulation intentionnelle du service

PARTIE 2 :

LE RÈGLEMENT EUROPÉEN SUR L'IA

Règlement européen sur l'IA



Journal officiel
de l'Union européenne

FR
Série L

2024/1689

12.7.2024

RÈGLEMENT (UE) 2024/1689 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 13 juin 2024

établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,
vu le traité sur le fonctionnement de l'Union européenne, et notamment ses articles 16 et 114,
vu la proposition de la Commission européenne,
après transmission du projet d'acte législatif aux parlements nationaux,
vu l'avis du Comité économique et social européen ⁽¹⁾,
vu l'avis de la Banque centrale européenne ⁽²⁾,
vu l'avis du Comité des régions ⁽³⁾,

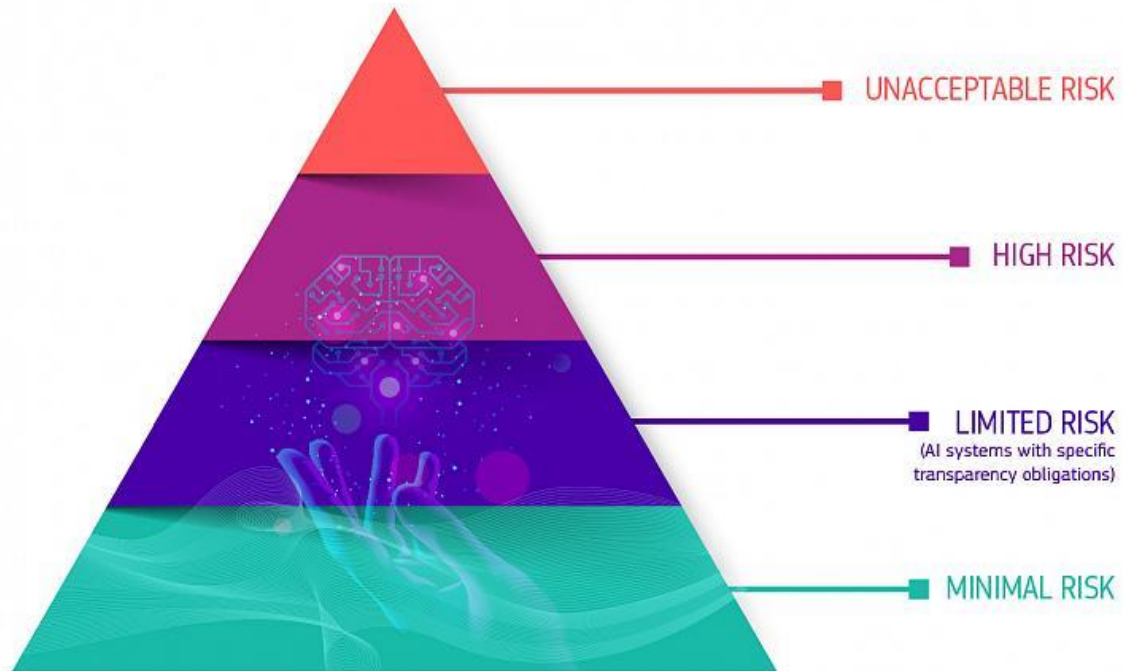


Certification obligatoire de
certains systèmes d'IA avant
leur mise sur le marché

Définition du système d'IA

« un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels »

La logique du niveau de risque à l'usage



Utilisations de systèmes d'IA interdites



Systèmes d'IA visés principalement par le règlement



Quelques obligations spécifiques



Aucune obligation
Contrainte volontaire

Les niveaux de risques des systèmes d'IA



Risques innacceptables – Utilisations de systèmes d'IA interdites

- 1) L'altération inconsciente du comportement d'un individu par des techniques subliminales
- 2) Exploitation des vulnérabilités (âge, handicap physique et mental) pour altérer le comportement d'un individu
- 3) Notation sociale qui entraîne 1) des sanctions dans un contexte différent de la collecte de données ou 2) une aggravation disproportionnée des sanctions
- 4) Identification biométrique à distance et en « temps réel » dans des espaces public*

Les niveaux de risques des systèmes d'IA



Risque haut/élevé – Les systèmes d'IA réglementés

1

Systèmes d'IA intégrés dans un produit déjà réglementé spécifiquement

OU

2

Utilisation d'un système d'IA dans un secteur critique

Les systèmes d'IA à haut risque sont les principales produits encadrés par le règlement européen sur l'IA

Liste des secteurs critiques



Activités des autorités répressives



Identification biométrique et catégorisation des personnes*



Accès et droit aux services privés essentiels et services publics



Gestion et exploitation des infrastructures critiques



Gestion migration, asile et contrôle aux frontières



Education et formation professionnelle

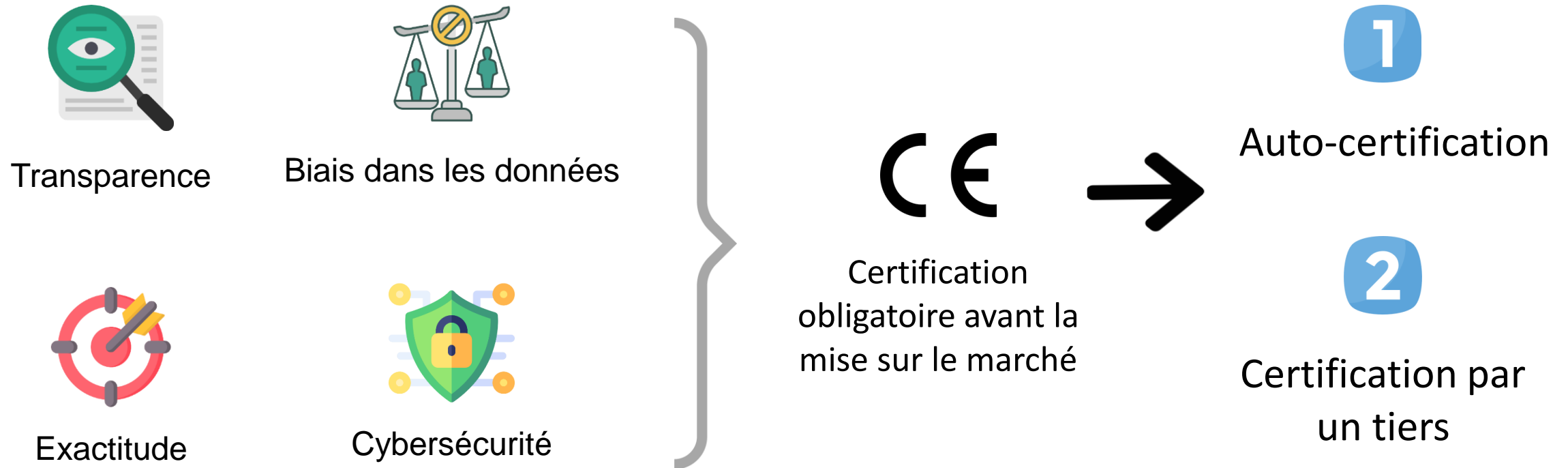


Administration de la justice et des processus démocratiques



Emploi, gestion main-d'œuvre et accès à l'emploi indépendant

Quelques obligations pour les fournisseurs de systèmes d'IA à haut risque



Sanctions en cas de manquement

- 1** Utilisation de SIA interdits, ou
Manquement aux obligations sur les données → 30M € ou 6% du CA annuel mondial
- 2** Manquement aux obligations du règlement → 20M € ou 4% du CA annuel mondial
- 3** Communication de fausses informations ou
d'informations trompeuses aux autorités → 10M € ou 2% du CA annuel mondial

Des questions ?



ÉVALUATION

Procès fictif



Reconstitution de décisions judiciaires emblématiques du droit du numérique



Equipes

- 3 personnes pour les avocats du « demandeur »
- 3 personnes pour les avocats du « défendeur »
- 5 personnes pour les juges de l'affaire



Déroulé

1. Arguments de la partie demanderesse (15 min)
2. Arguments de la partie défenderesse (15 min)
3. Questions des juges (30 min)
4. Conclusion de la partie demanderesse (5 min)
5. Conclusion de la partie défenderesse (5 min)

Les parties

Arguments des parties :



- Qui représentez-vous ?
- Quels sont les points principaux de votre demande / défense
- Quelles sont les preuves légales qui confirment votre propos ?
- Il y a-t-il des réglementations / décisions antérieures qui supportent votre argumentaire ?
- Quel est l'argumentaire de la partie opposée ?
- Pourquoi est-ce votre propos qui est correct plutôt que le leur ?

Conclusion des parties :



- Résumé des arguments principaux
- Prise en compte des questions posées par les juges
- Adaptation aux arguments de la partie adverse

Les juges



- Poser les questions tour à tour
- Gestion du temps de parole des parties
- Modération des discussions



- Aide à clarifier un argument présenté
- Développe les points de vue des deux parties
- Expose les concepts et définitions pendant la décision



Les juges ne doivent prendre leur décision qu'à partir des arguments énoncés par les parties !

Barème d'évaluation

Barème des parties :

Clarté	Clarté de l'argumentaire	5
Compréhension	Démontre une bonne compréhension des enjeux, de l'affaire	5
Réponse aux questions	Répond aux questions clairement et montre sa préparation	5
Conclusion adaptée	Intègre et répond à l'argumentaire de la partie opposée dans la conclusion	5

Barème d'évaluation

Barème des juges :

Préparation des questions	Montre sa préparation en posant des questions adaptées et pertinentes	5
Gestion de la discussion	Clarifie la question lors d'une réponse partielle, demande aux parties de réfuter, encourage la discussion, gère les temps de réponse	5
Décision adaptée	La décision écrite résume les arguments et est pertinente avec ce qui a été entendu au procès	5
Décision comparée	La décision écrite est comparée à la décision réelle de façon claire	5

Affaires pour les procès fictifs

1. Ligue des droits humains v. Conseil des ministres, Affaire [C-817/19](#) (dit PNR)
2. NJCM et al. v. State, The Hague Distric Court
[ECLI:NL:RBDHA:2020:1878](#) (dit SyRI)
3. Meta Platforms Inc. v. Bundeskartellamt, Affaire [ECLI:EU:C:2023:537](#)
4. ND v. DR, Affaire [ECLI:EU:C:2024:846](#)

Entrainement : Analyse d'arrêt

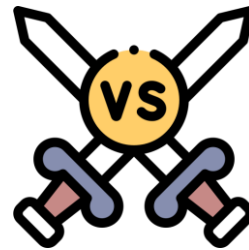


Arrêt de la Cour de justice de l'Union européenne

Rendu le 13 mai 2014, Numéro de décision : [C-131/12](#)



Mario Costeja González



Google

MERCI DE VOTRE
ATTENTION !