

ISAE-SUPAERO



LE DROIT DES DONNÉES PERSONNELLES

Mélanie Gornet, Télécom Paris
melanie.gornet@telecom-paris.fr

Programme

Aujourd'hui (mercredi 6 mars)

Matin

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

Après-midi

- Résumé d'autres lois européennes sur le numérique (45min)
- Présentation des modalités d'évaluation (15min)
- Cas d'étude : Google Spain (2h)

La semaine prochaine (vendredi 15 mars)

Evaluation : procès fictifs

Importance de la donnée

**Les données personnelles :
le pétrole du 21ème siècle**



Refuser et s'abonner pour 1€ →

Soutenez [redacted] ! Dites oui

Nous et nos partenaires utilisons des technologies comme les cookies pour stocker et/ou accéder à des informations personnelles non sensibles stockées sur votre terminal (identifiants uniques, ...), que nous traitons afin de réaliser des statistiques d'usage du site, personnaliser les publicités et le contenu et en mesurer les performances, produire des données d'audience, développer et améliorer les produits. Ces technologies peuvent utiliser des données de géolocalisation précises ou analyser activement les caractéristiques du terminal pour l'identification.

Cliquez sur le bouton « Oui, j'accepte » pour consentir à ces utilisations sur ce site, sur « Paramétrages » pour paramétrer vos choix et/ou vous opposer lorsque l'intérêt légitime est utilisé ou sur « Refuser et s'abonner pour 1€ ».

Vous pouvez à tout moment revenir sur vos choix en utilisant le lien « Paramétrages » disponible dans notre page de gestion des cookies.

Oui, j'accepte

Paramétrages

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

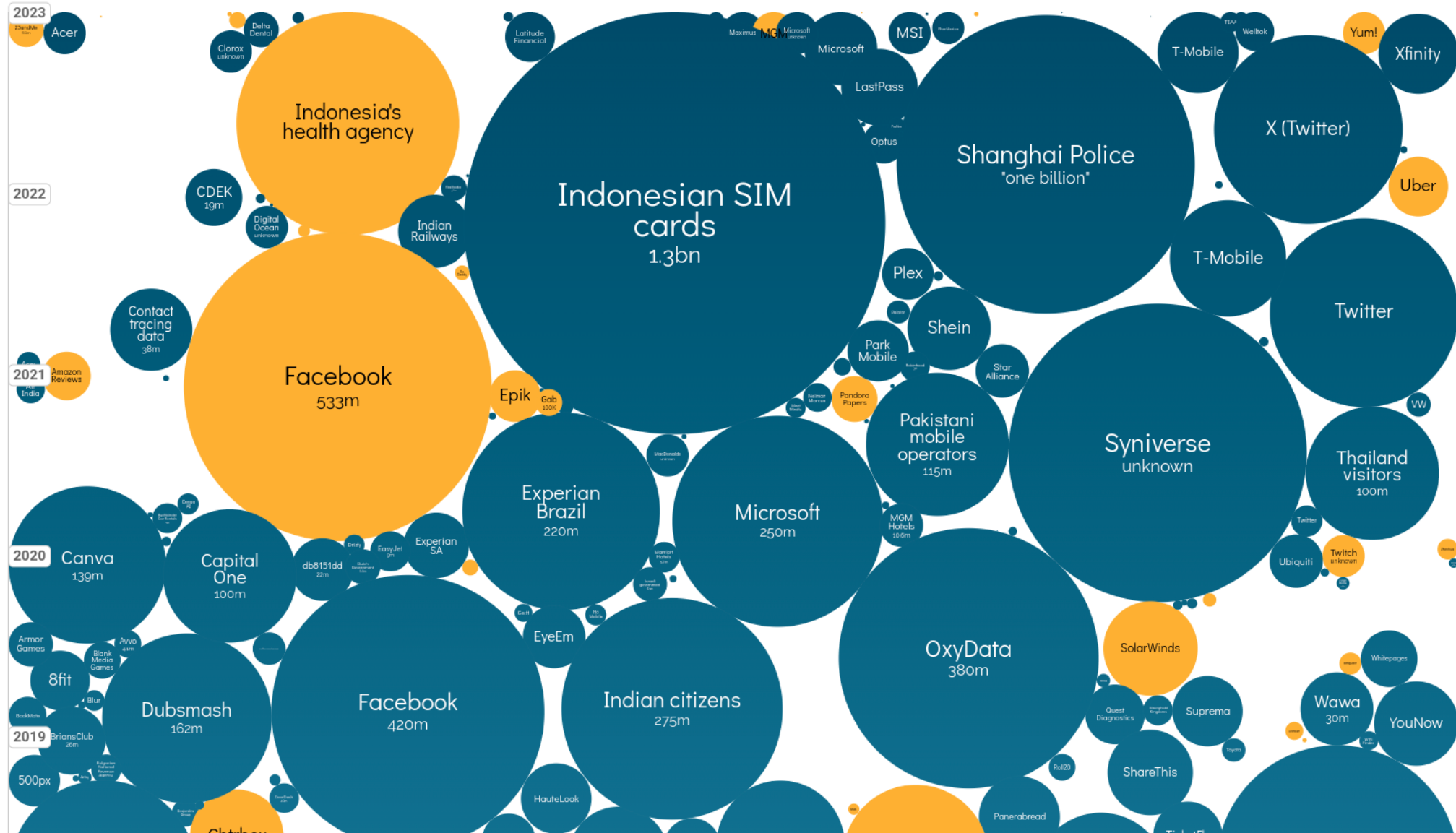
Pendant la campagne électorale de 2016, la campagne de Donald Trump aurait fait main basse sur les données de cinquante millions d'utilisateurs.

Scandale Cambridge Analytica -
Facebook



« Derrière nos écrans de fumée », Netflix
([Bande annonce](#))

Enjeux de sécurité des données



World's Biggest Data Breaches & Hacks ([lien](#))

Le droit à la vie privée



Capitalisme de surveillance,
Shoshanna Zuboff ([vidéo](#))



*« 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](#), [film](#))

Historique international et européen 1/2

- 1980 : OCDE Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel ([lien](#))

7 principes :

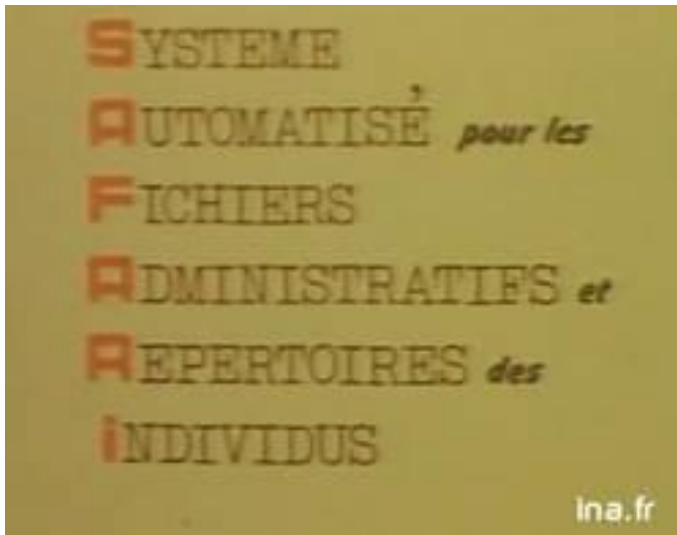
- limitation en matière de collecte
 - qualité des données
 - limitation de l'utilisation
 - garanties de sécurité
 - participation individuelle
 - responsabilité
- 1981 : Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ([lien](#))

Historique international et européen 2/2

- 1995 : Directive 95/46/CE sur la protection des données personnelles ([lien](#))
- 2000 : Charte des Droits Fondamentaux de l'Union Européenne ([lien](#))
- 2012 : Groupe de travail « article 29 », Avis 01/2012 sur les propositions de réforme de la protection des données ([lien](#))
- 2016 : Règlement UE 2016/679 sur la protection des données (RGPD) ([lien](#))
- 2018 : entrée en vigueur du RGPD

Historique français de la réglementation 1/2

Le projet SAFARI



... LE MONDE — 21 mars 1974 — Page 9

JUSTICE

Tandis que le ministère de l'intérieur développe la centralisation de ses renseignements

Une division de l'informatique est créée à la chancellerie

En ordre dispersé, les départements ministériels tentent de développer à leur profit, à leur seul usage, l'informatique et son outil, l'ordinateur. Ce n'est pas tout à fait un hasard si, à l'époque où le Journal officiel va publier un arrêté créant une « division de l'informatique » au ministère de la Justice, celui de l'intérieur met la dernière main à la mise en route d'un ordinateur

puissant destiné à rassembler la masse énorme des renseignements grattés sur tout le territoire; pas un hasard non plus si le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) destiné à définir chaque Français par un « identifiant », qui ne définit pas que lui, maintenant terminé, est l'objet de convoitises ardentes: le ministère de l'intérieur y souhaite

jouer le premier rôle. En effet, une telle banque de données, sous-jacent opérationnel de toute autre collecte de renseignements, donnera à qui la possèdera, une puissance sans égale.

Ainsi se trouve d'évidence posé un problème fondamental, même s'il est rebattu: celui des rapports des libertés publiques et de l'informa-

tique. Son importance exigerait qu'il en soit, au Parlement, publiquement débattu. Tel ne paraît pas être, pourtant, la solution envisagée par le premier ministre dans les directives qu'il vient d'adresser au ministère de la Justice, intéressé au premier chef si l'on s'en rapporte à la Constitution qui dans son article 66 fait de l'autorité judiciaire le gardien des libertés individuelles.

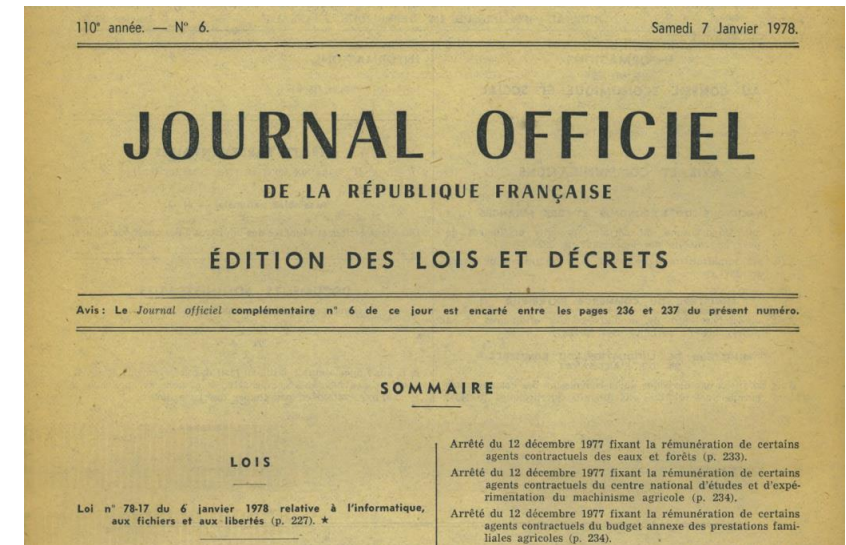
- 1970 : le député Michel Poniatowski propose à l'Assemblée nationale la création d'un comité de surveillance et d'un tribunal de l'informatique, la suggestion est rejetée
- 1971 : Projet SAFARI d'interconnexion de fichiers nominatifs
 - Centralisation des données
 - Utilisation du NIR pour vérifier l'identité des personnes
 - Faciliter les études statistiques de la population
- 1974 : Révélation du projet par le journal *Le Monde*

« Safari » ou la chasse aux Français

Historique français de la réglementation 2/2

La Loi Informatique et Libertés

- 1978 : Première version de la LIL après le scandale du projet SAFARI
 - Création d'une autorité nationale de protection des données personnelles
- 2004 : réforme de la LIL pour la transposition libre de la Directive de 95
 - « informations nominatives » devient « données à caractère personnel »
 - accroît les pouvoirs de la CNIL pour les contrôles et les sanctions
- Déc 2018 : mise en cohérence de la LIL avec le RGPD ([lien](#))



CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

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



- Voté en 2016 et entré en vigueur le 25 Mai 2018, remplace la directive européenne de 1995 ([lien](#))
- Intégré à un paquet européen
- Logique de mise en conformité
- 2 objectifs :
 - Protéger les données personnelles
 - Permettre la libre circulation des données au sein de l'Union
- Application large
- Sanctions très importantes en cas de violation
- Un texte qui a fait école

I. Champ d'application

1. Champ d'application matériel → « quoi »
2. Champ d'application territorial → « où »
3. Champ d'application personnel → « qui »

Qu'est-ce qu'une donnée personnelle ?



Nom / Prénom



Photos satellites



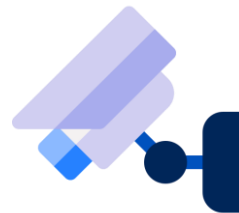
Numéro de
téléphone d'une
entreprise



Adresse email
professionnelle



Régime alimentaire
d'un client



Enregistrement
vidéosurveillance

Une adresse IPv4 (notation décimale à point)

172 . 16 . 254 . 1

Adresse IP

La notion de donnée à caractère personnel

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

Art. 4.1 RGPD

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 de :

- L'origine raciale ou ethnique ;
- L'opinion politique ;
- Les convictions religieuses ou philosophiques ;
- L'appartenance syndicale ;
- Les données génétiques ou biométriques ;
- Les données de santé ;
- La vie sexuelle ou orientation sexuelle ;

→ Ne peuvent pas faire l'objet d'un traitement (sauf exception)

Art. 9 RGPD

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 »

Art. 4.2 RGPD

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 !

Les personnes redevables



Responsable(s)
de traitement

- **Choisit les finalités et les modalités** du traitement Art. 4.7 RGPD
- **Maîtrise intellectuelle** du traitement
- **Responsabilité** civile et pénale en cas de manquement



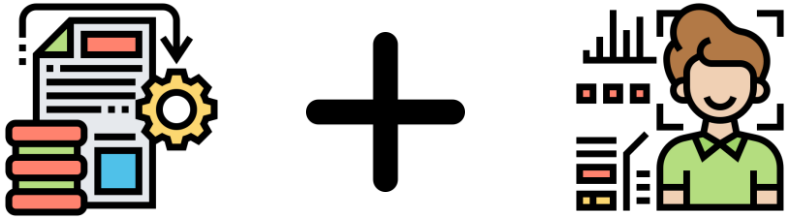
Sous-traitant

- Traite les données **pour le compte du responsable** de traitement Art. 4.8 RGPD
- **Maîtrise technique** du 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

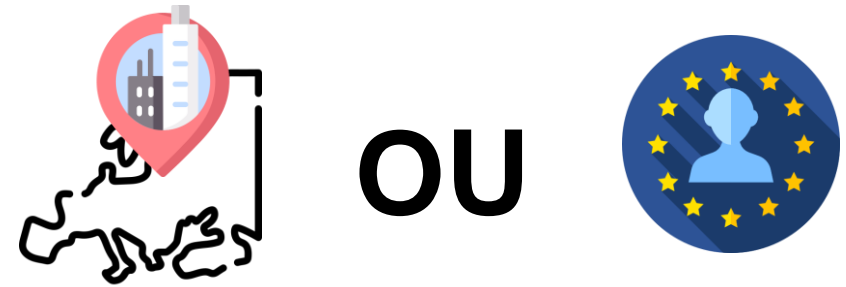
Champ d'application matériel



Présence d'un traitement de données à caractère personnel

Art. 2 RGPD

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

Art. 3 RGPD

II. Régime → « comment »

1. Les obligations
2. Les droits

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**



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 !

Art. 5.1 RGPD

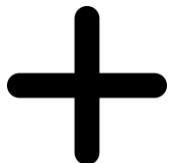
Conséquences : Toutes vos actions sur les données doivent être proportionnelles avec les finalités → principe de **minimalisation** des données



- 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 pour traitement ultérieur (sauf exceptions)

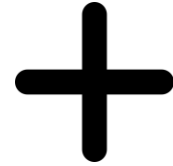


Principe de **loyauté** et de **transparence** : la personne concernée doit savoir que ses données font l'objet d'un traitement et doit connaître la finalité du traitement

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 1/3

RAPPEL

Si les données proviennent d'européens 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 2/3

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 3/3

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.

Art. 45 RGPD

L'exemple des Etats-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 :

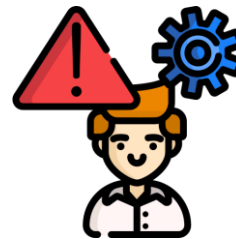


- Chiffrement
- Mot de passe sécurisé
- Eviter le BYOD
- Back up régulier ...

→ principe de **sécurité**

2 Après la faille de sécurité

- Notification à l'autorité de contrôle dans les plus brefs délais
- 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

→ principe d'**information**

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



- Récupérer les données que **vous avez fournies** à la plateforme
- Transférer ces données d'une plateforme à l'autre

Remarque : Les données sont dans un **format lisible par la machine**.

- Effacer ou déréférencer des données personnelles vous concernant
- Exemples : photos ou liens gênants

Remarque : ce droit ne s'applique que dans **certaines situations**. Pensez à vous renseigner avant de faire la demande

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 »

III. Les organes de contrôle, les recours et les sanctions

→ « par qui »

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 ;

Les Autorité de Contrôle Indépendantes

Au moins une par état membre. En France, la 

- **Informe** les acteurs de leurs obligations (mission de sensibilisation) ;
- **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

Autres organes de contrôle

Le Contrôleur Européen de la Protection des Données (EDPS)

Autorité de contrôle indépendante des institutions européennes (par exemple la Commission européenne) sur la protection des données

Comité Européen de la Protection des Données (EDPB)

Comprend :

- les chefs des autorités de l'autorité de contrôle de chaque État membre, ou leurs représentants.
- le Contrôleur européen de la protection des données, ou leurs représentants.

Veille notamment à la cohérence des pratiques et des sanctions des autorités

Recours possibles



- Recours devant une autorité de contrôle (dépôt de plainte en ligne sur le site de la CNIL)

- Recours judiciaire



- Sanction administrative

- Sanction judiciaire



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 France

Déc
2018



Sécurité des données des
clients insuffisante



400.000 €

Jan
2019



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



50.000.000 €

Déc
2021



150.000.000 €












Jan
2024



Surveillance de performance +
conservation données
disproportionnée

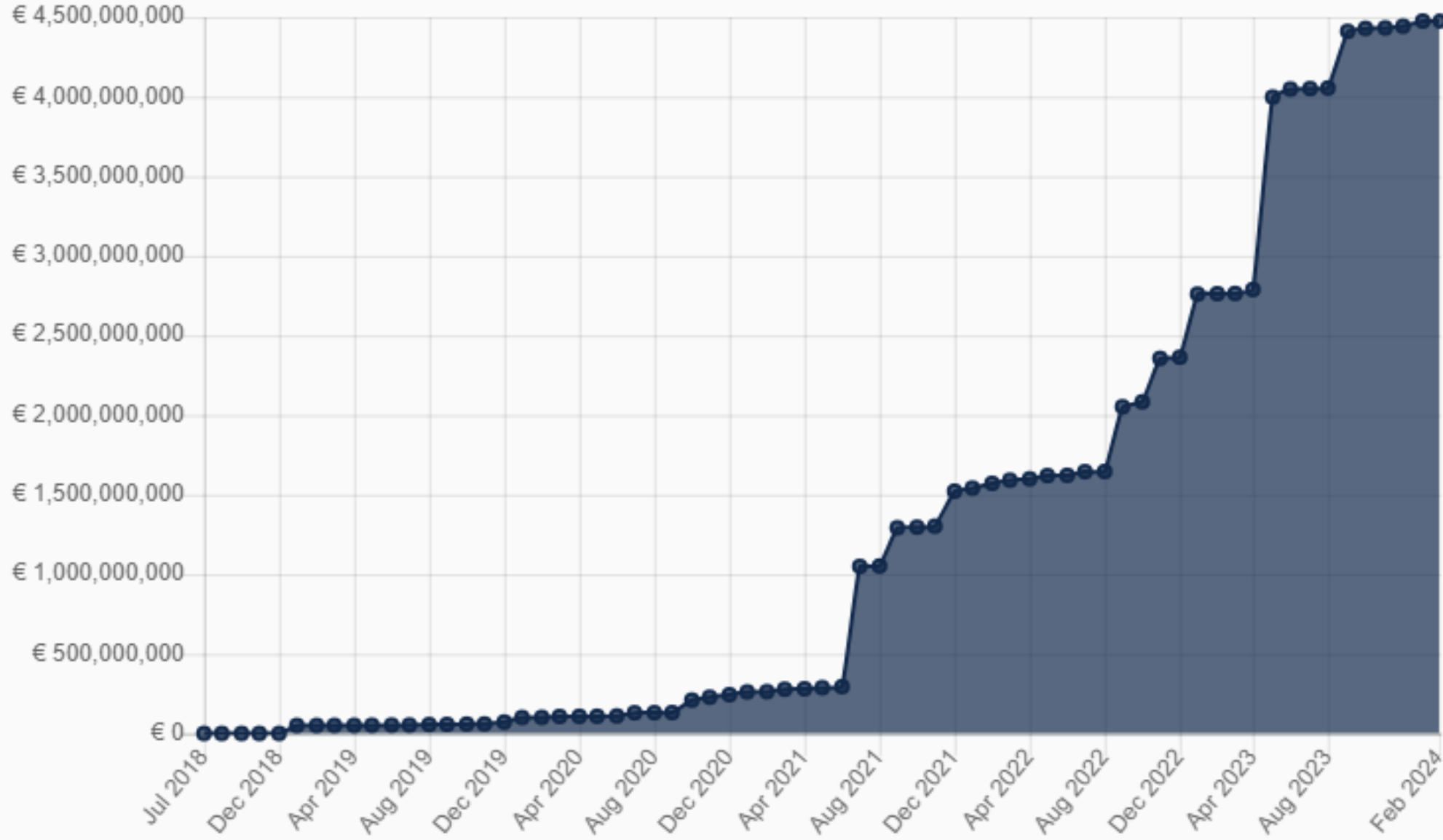


32.000.000 €

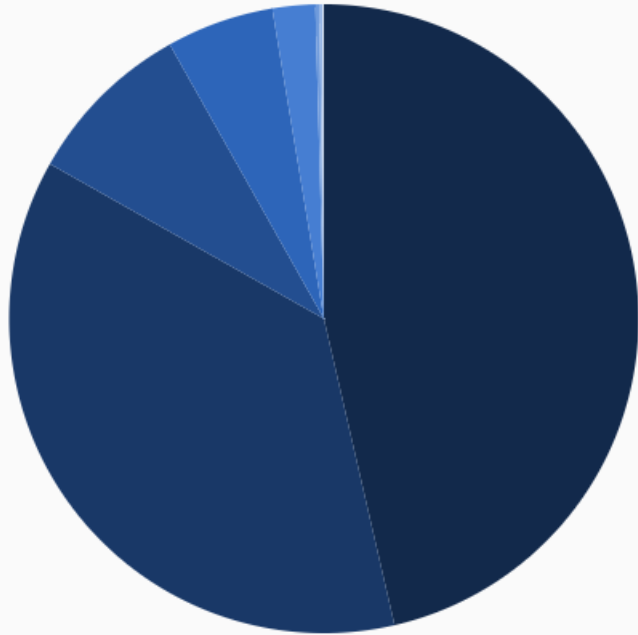
Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type
 IRELAND	2023-05-12	1,200,000,000	Meta Platforms Ireland Limited	Art. 46 (1) GDPR	Insufficient legal basis for data processing
 LUXEMBOURG	2021-07-16	746,000,000	Amazon Europe Core S.à.r.l.	Unknown	Non-compliance with general data processing principles
 IRELAND	2022-09-05	405,000,000	Meta Platforms, Inc.	Art. 5 (1) a), c) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 24 GDPR, Art. 25 (1), (2) GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
 IRELAND	2023-01-04	390,000,000	Meta Platforms Ireland Limited	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR, Art. 12 GDPR, Art. 13 (1) c) GDPR	Non-compliance with general data processing principles
 IRELAND	2023-09-01	345,000,000	TikTok Limited	Art. 5 (1) c), 5 (1) f) GDPR, Art. 12 (1) GDPR, Art. 13 (1) e) GDPR, Art. 24 (1) GDPR, Art. 25 (1), (2) GDPR	Non-compliance with general data processing principles
 IRELAND	2022-11-25	265,000,000	Meta Platforms Ireland Limited	Art. 25 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security
 IRELAND	2021-09-02	225,000,000	WhatsApp Ireland Ltd.	Art. 5 (1) a) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient fulfilment of information obligations
 FRANCE	2021-12-31	90,000,000	Google LLC	Art. 82 loi Informatique et Libertés	Insufficient legal basis for data processing
 FRANCE	2021-12-31	60,000,000	Facebook Ireland Ltd.	Art. 82 loi Informatique et Libertés	Insufficient legal basis for data processing
 FRANCE	2021-12-31	60,000,000	Google Ireland Ltd.	Art. 82 loi Informatique et Libertés	Insufficient legal basis for data processing
 FRANCE	2019-01-21	50,000,000	Google LLC	Art. 13 GDPR, Art. 14 GDPR, Art. 6 GDPR, Art. 5 GDPR	Insufficient legal basis for data processing

(Source)

a) Course of overall sum of fines (cumulative):



1. By total sum of fines:



Violation	Sum of Fines
Non-compliance with general data processing principles	€ 2,079,844,659 (at 560 fines)
Insufficient legal basis for data processing	€ 1,649,422,112 (at 620 fines)
Insufficient technical and organisational measures to ensure information security	€ 388,458,875 (at 360 fines)
Insufficient fulfilment of information obligations	€ 247,481,060 (at 187 fines)
Insufficient fulfilment of data subjects rights	€ 98,366,170 (at 194 fines)
Unknown	€ 9,250,000 (at 9 fines)
Insufficient cooperation with supervisory authority	€ 6,205,529 (at 108 fines)
Insufficient fulfilment of data breach notification obligations	€ 1,813,282 (at 35 fines)
Insufficient data processing agreement	€ 1,057,110 (at 11 fines)
Insufficient involvement of data protection officer	€ 955,300 (at 20 fines)

Cet après-midi...



Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

**LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE
(ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION
LEGISLATIVE ACTS**

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

Cet après-midi...



« Costeja González, l'homme qui a fait plier Google » ([Source](#))

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González

[ECLI:EU:C:2014:317](#) (disponible dans d'autres langues [ici](#))

- Portée géographique des lois européennes sur la protection des données
- Droit à l'effacement dans les bases de données
- Définition traitement de données et du responsable du traitement



Jurisprudence pré-RGPD

Des questions ?



The image features a central globe with a glowing blue and red circuit board pattern overlaid on it. The globe is surrounded by a ring of twelve yellow stars, reminiscent of the European Union flag. The text "AI Act et autres initiatives" is written in white, sans-serif font across the center of the globe.

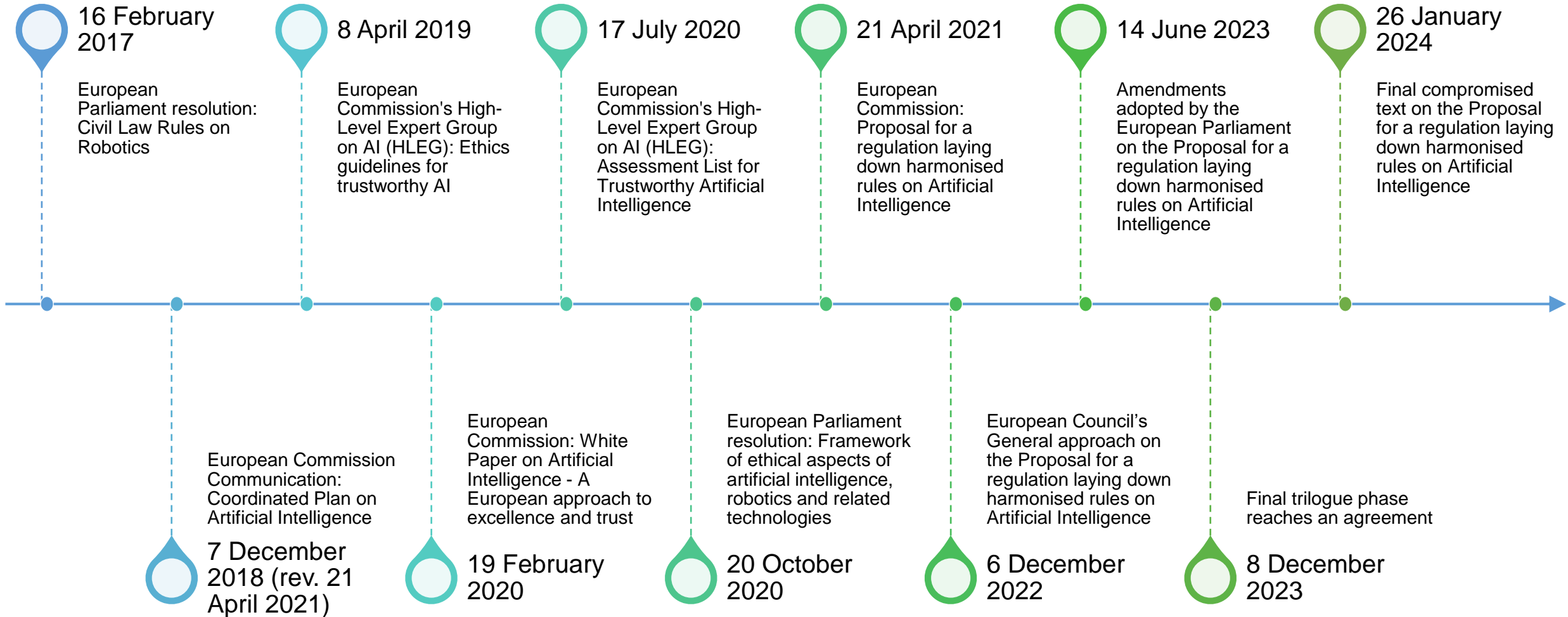
AI Act et autres initiatives

Règlement sur l'intelligence artificielle (AI Act)



- Voté en décembre 2023 et entré en vigueur prévue en 2025
- Intégré à un paquet européen
- Logique de mise en conformité
- 2 objectifs :
 - Protéger les utilisateurs de systèmes d'IA
 - Permettre la libre circulation des systèmes d'IA au sein de l'Union

Context of the AI Act



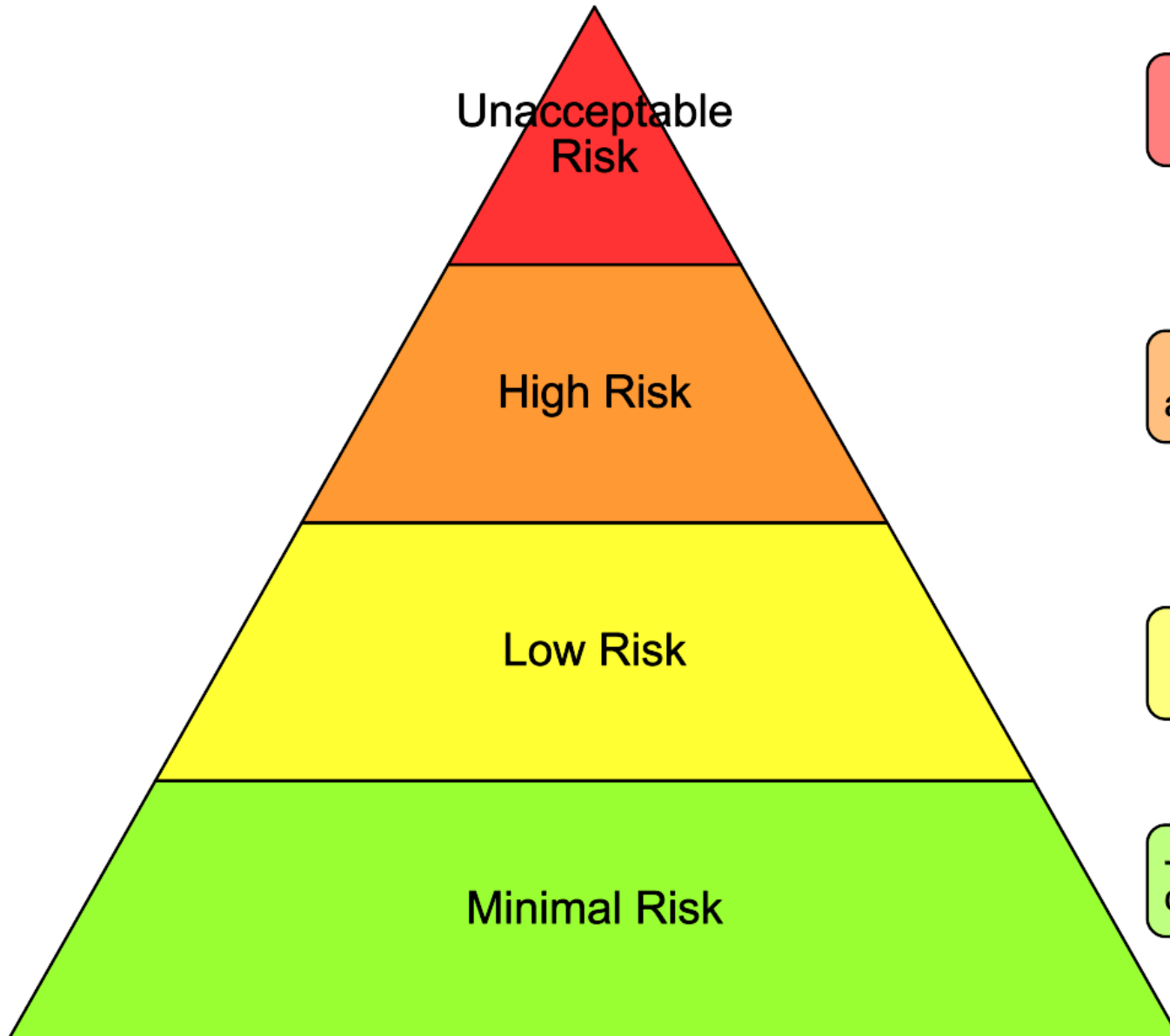
Definition of AI

‘**AI system**‘ is a **machine-based system** designed to operate with varying **levels of autonomy** and that may exhibit **adaptiveness** after deployment and that, for explicit or implicit objectives, **infers, from** the **input** it receives, how to generate outputs such as *predictions, content, recommendations, or decisions* that can **influence** physical or virtual **environments**;

Multitudes of definitions

Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
<p>(1) ‘artificial intelligence system’ (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;</p> <p style="text-align: center;"><u>ANNEX I</u> <u>ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES</u> <u>referred to in Article 3, point 1</u></p> <p>(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;</p> <p>(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;</p> <p>(c) Statistical approaches, Bayesian estimation, search and optimization methods.</p>	<p>(1) ‘artificial intelligence system’ (AI system) means software a machine-based system that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as content, predictions, recommendations, or decisions that</p>	<p>(1) ‘artificial intelligence system’ (AI system) means software a system that is developed with one or more of the techniques and approaches listed in Annex I and can, for designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of human-defined objectives, generate objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations, or decisions, influencing the environments they interact with with which the AI system interacts;</p>	<p>(1) ‘artificial intelligence An AI system’ (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as content, predictions, content, recommendations, or decisions influencing the that can influence physical or virtual environments. they interact with;</p>

Risk-based classification



Art. 5: Prohibited use

- Ex: subliminal techniques, biometric categorisation on sensible attributes, social scoring, real-time remote biometric identification in public spaces by law enforcement, prediction of criminal offences, ...

Art. 6 et seq: Strict obligations & Conformity assessment

- Ex: machinery, toys, medical devices, aviation, remote biometric identification, biometric categorisation, critical infrastructure, education, employment, essential services (healthcare, credit, emergency, insurance), border control...

Art. 52: Transparency obligations

- Ex: general purpose AI, chatbots, deep fakes, emotion recognition...

-: Product safety rules & voluntary code of conduct

- Ex: video games, spam filters...

Requirements for high-risk systems

- Risk management system
- Data and data governance
- Technical documentation
- Record keeping
- Transparency and provision of information to deployers
- Human oversight
- Accuracy, robustness and cybersecurity

CE marking



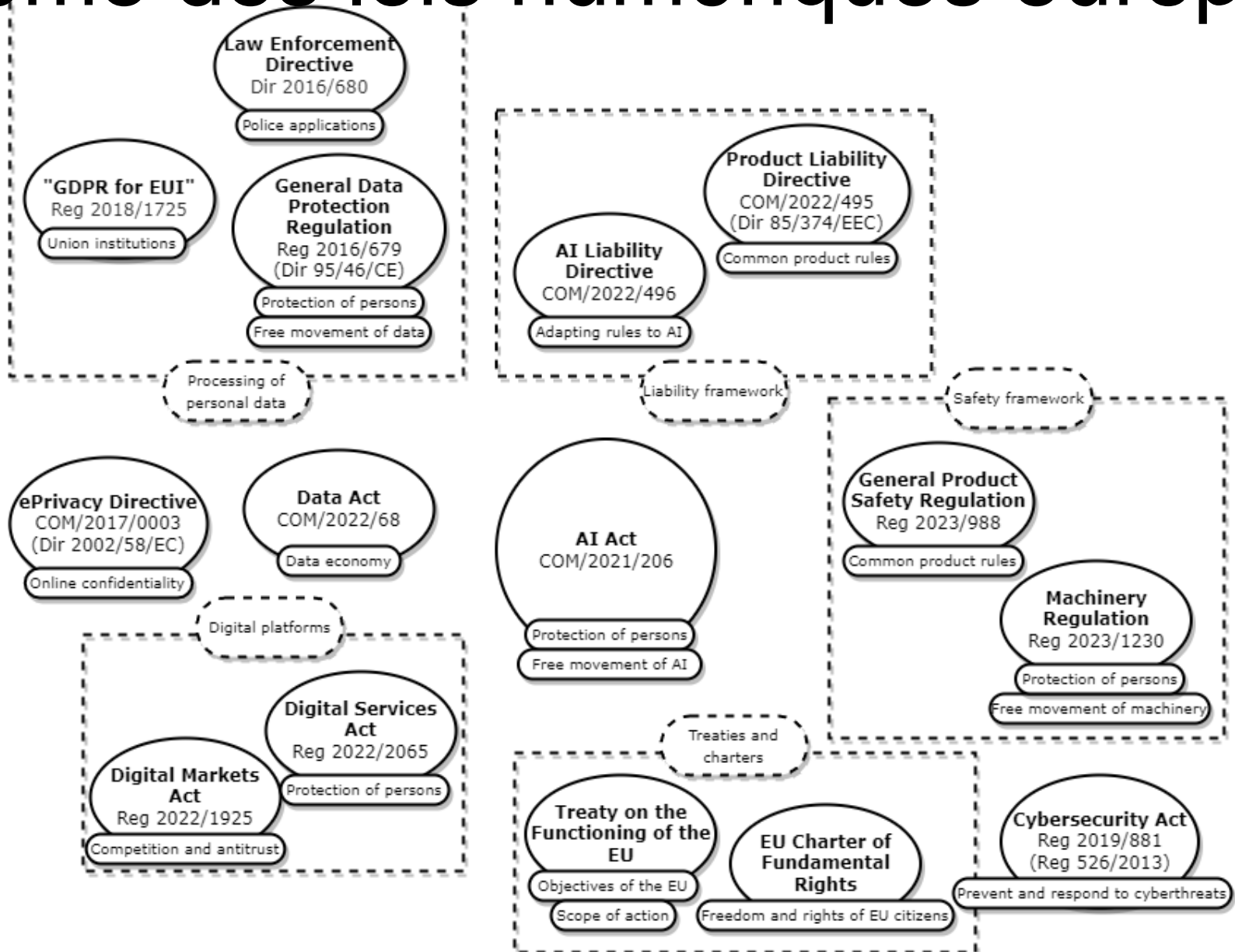
The product manufacturer:

- Identifies the applicable directive(s) and harmonised standard
- Verifies the product specific requirements
- Identifies whether an independent conformity assessment (by a notified body) is necessary
- Tests the product and check its conformity
- Draws up and keeps available the required technical documentation
- Affixes the CE marking and draws up the EU declaration of conformity

Quelques points de tension

- Biometrics
- General purpose AI
- Generative AI
- High-impact capabilities models
- Open source

Ecosystème des lois numériques européennes



Digital Markets Act (DMA)

- **Entré en vigueur** : mai 2023
- **But** : compléter le droit à la concurrence pour éviter le monopole des très grandes plateformes (réseaux sociaux, navigateurs web...)

Champ application

- Plateformes de services essentiels
- CA ou valorisation boursière élevée
- Grand nombre d'utilisateurs en EU

Obligations

- Faciliter désabonnement et interopérabilité avec concurrents
- Interdiction d'auto-préférence
- Réutilisation de données à caractères personnelles pour publicités ciblées seulement sous consentement
- Informer des fusions...

Digital Services Act (DSA)

- **Entré en vigueur** : août 2023
- **But** : harmonisation des réglementations sur les contenus et produits illicites (haine, pédoporno, terroriste, désinformation, drogues, contrefaçons...)

Champ application

- Fournisseur d'accès à internet
- Services cloud
- Plateformes en ligne

Obligations

- Outils signalisation
- Traitement des réclamations
- Explication des algorithmes
- Interdiction publicités ciblées sur mineurs
- Analyse de risques et audits annuels
- Accès (limité) à l'interface

Data Act

- **Entrée en vigueur** : janvier 2024
- **But** : faciliter le partage des données en Europe

Champ application

- données industrielles
- IoT

Contenu

- Rendre accessible les données des appareils connectés
- Si besoin exceptionnel, utilisation des données des entreprises par organismes publics
- Suppression des frais de changement de fournisseurs de services
- Normes d'interopérabilité
- Garanties contre accès illicites de gouvernements de pays tiers

Evaluation



Procès fictif

Pour l'évaluation de ce cours, vous reconstituerez des cas de **jurisprudence** emblématiques de la protection des données.

Pour chaque procès, vous serez organisés en **3 équipes** :

- 5 personnes pour l'équipe « demandeur »
- 5 personnes pour l'équipe « défendeur »
- 5 juges

Le procès se déroulera comme suit :

- 15min arguments des demandeurs
- 15min arguments des défendeurs
- 30min de questions par les juges (15min de réponse par partie)
- 5min de conclusion des demandeurs
- 5min de conclusion des défendeurs

Arguments oraux 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 ?

Questions des juges

Les juges posent leurs questions tour à tour. Les demandeurs et défendeurs ont 15min chacun pour répondre. Les juges sont responsables de préparer des bonnes questions, gérer le temps, modérer la discussion.

Une bonne question :

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

Les juges ne doivent pas pénaliser les autres équipes si elles ne connaissent pas des détails particuliers de l'affaire, d'affaires liées ou du droit des données mais doivent construire à partir de la préparation de chaque équipe une discussion utile pour la décision finale.

Les demandeurs et défendeurs doivent préparer des supports clairs et facilement accessibles pour répondre au mieux aux questions.

Conclusions des parties

5min de conclusion pour les demandeurs et 5min pour les défendeurs.

La conclusion doit résumer les arguments principaux, prendre en compte les arguments de la partie adverse et les questions posées.

Il est conseillé de préparer un brouillon en avance et de le modifier au fur et à mesure du procès.

Décision

Une semaine après le procès, les juges doivent rendre une décision écrite (1-2 pages) expliquant les arguments des deux parties, la décision prise et pourquoi cette décision.

Le document doit inclure la décision globale de l'affaire, les pénalités perçues par l'une ou l'autre des parties, les définitions éventuelles auxquelles la décision permet d'aboutir (ex notion de responsable du traitement dans l'affaire Google Spain) ainsi que les implications pour les cas futurs.

La décision sera basée sur les arguments oraux exposés en cours ainsi que les réponses aux questions des juges. Mais elle doit aussi inclure une comparaison à la décision de l'affaire réelle.

Il est recommandé de séparer les juges en deux groupes de 3 : un groupe pour la préparation des questions et un pour l'écriture de la décision.

Planning

Organisation par équipes d'ici la fin de la journée.

Cet après-midi : cas Google Spain, exemple de préparation d'un procès fictif.

Procès fictifs en classe le 15/03/2024. 1h10 pour chaque procès, 2 blocs dans 2 salles en parallèle.

Décisions écrites sur le LMS pour le 22/03/2024.

Evaluation par les pairs : les élèves du bloc 1 notent ceux.elles du bloc 2 et vice-versa.

Grille de notation : demandeur / défendeur

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

Grille de notation : 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, Case [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, Case [ECLI:EU:C:2023:537](#)
4. Affaire « La Quadrature du Net », Tribunal administratif de Marseille N°[1901249](#), Rapport d'informations au Sénat N°[627 \(2021-2022\)](#)

Des questions ?

