Intervention de Jonathan KELLER, Institut Mines Télécom Paris, le 8/11/2022 à Saint-Etienne

Compte-rendu par des participants

Cas d'étude : reconnaissance faciale appliquée à des personnes étrangères dans les gares

De quoi parle-t-on ?

- *Intelligence artificielle*
- *à vocation de reconnaissance faciale*
- *de visages de ressortissants étrangers*
- *dans les gares*

1. Complexité du droit applicable

2. Un contexte géopolitique particulier
Souverainisme européen contre domination technologique américaine
Tensions entre deux conceptions de l'Europe

3. La volonté de construction d'une réglementation numérique européenne
A. La protection (de l'industrie) européenne
B. Un secteur en plein essor: le capitalisme européen de la surveillance

4. L'AIA (Artificial Intelligence Act, Projet de règlement sur l'IA)
- Définition de l'intelligence artificielle et vision conceptuelle (SIA)
- Limites et cas d'interdiction
- Position des acteurs politiques

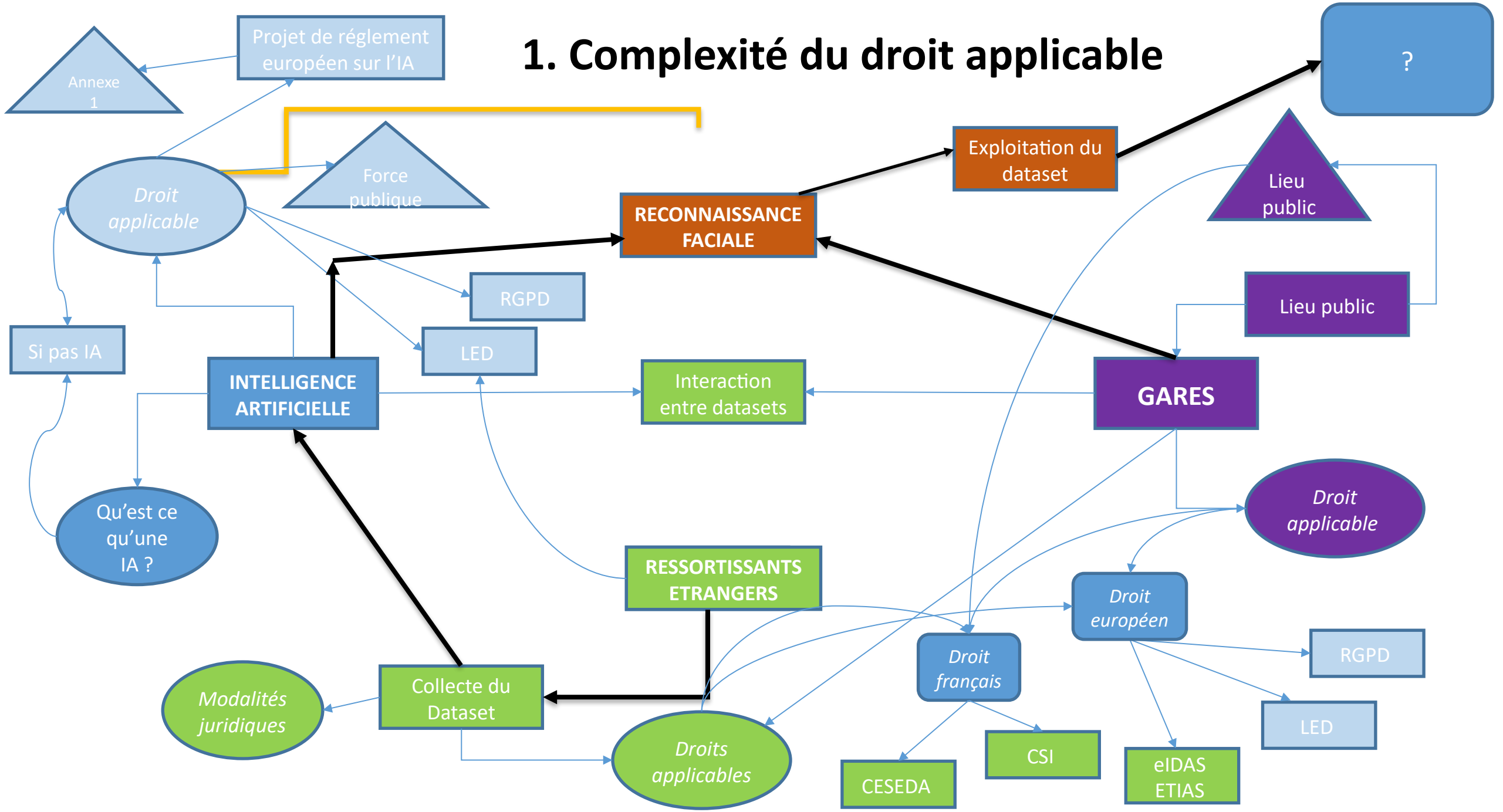
5. Flou juridique entre les polices judiciaire (qui se réfère au RGPD) et administrative (… au LED)

6. La reconnaissance faciale
- Définition selon les processus
- Définition selon les fonctions
- Exemples d'identification par reconnaissance faciale

7. Les justifications d'une ingérence étatique
A. Les étrangers comme béta-testeurs
B. Des zones sensibles à protéger

8. Résolution du cas

1. Complexité du droit applicable



Quelques définitions et sigles

Notion de datasets (ou jeux de données) : couramment utilisés en machine learning (apprentissage automatique), ils regroupent un ensemble de données cohérent qui peuvent se présenter sous différents formats (textes, chiffres, images, vidéos etc…). Chaque valeur présente dans un dataset est associée à un *attribut* et à une *observation*.

Ex pour des personnes étrangères : les attributs correspondront à différentes caractéristiques telles que l'âge, le poids, la taille, le pays d'origine… Alors que chaque observation sera associée à une personne différente.

Droit français

CESEDA : code de l'entrée et du séjour des étrangers et du droit d'asile

CSI : code de la sécurité intérieure. Il regroupe l'ensemble des dispositions législatives et réglementaires ayant trait à la sécurité intérieure

Droit européen

LED Code européen de bonne conduite administrative

RGPD Réglement général pour la protection des données

ETIAS : système européen d'autorisation et d'information concernant les voyages, pour les visiteurs exemptés de visa voyageant dans l'Union ou l'espace Schengen

EIDAS : règlement sur l'identification électronique et les « services de confiance » (chargés de vérifier l'identité d'origine et l'intégrité des messages échangés par Internet) pour les transactions électroniques au sein de l'Union Européenne.

2. Un contexte géopolitique particulier : souverainisme européen contre domination technologique américaine

- avant mars 2022 : l'arrêt Schrems (par la Cour de Justice de l'UE) a affirmé une souveraineté numérique européenne

« Les données personnelles des ressortissants européens doivent être protégées dans les mêmes conditions qu'en Europe »

- Depuis mars 2022, guerre avec la Russie

Les Etats-Unies soutiennent l'Europe par

- Le pétrole
- Les renseignements

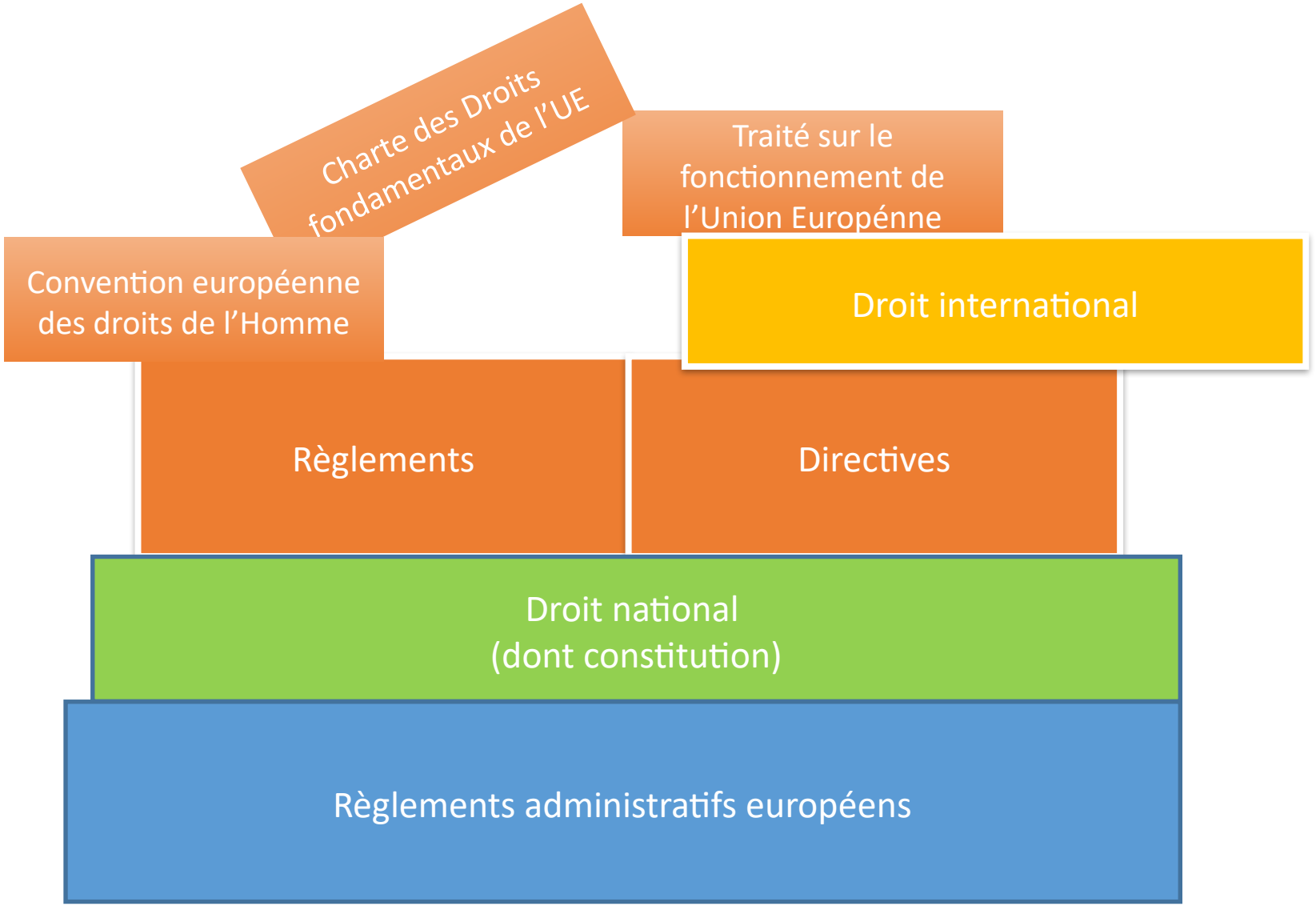
Mais pas sans contreparties

Demande de la remise en cause de Schrems et donc retour à la colonisation numérique européenne par les Etats-Unis

Le contexte martial et la crise migratoire entraînent aussi des questions sur le respect du droit

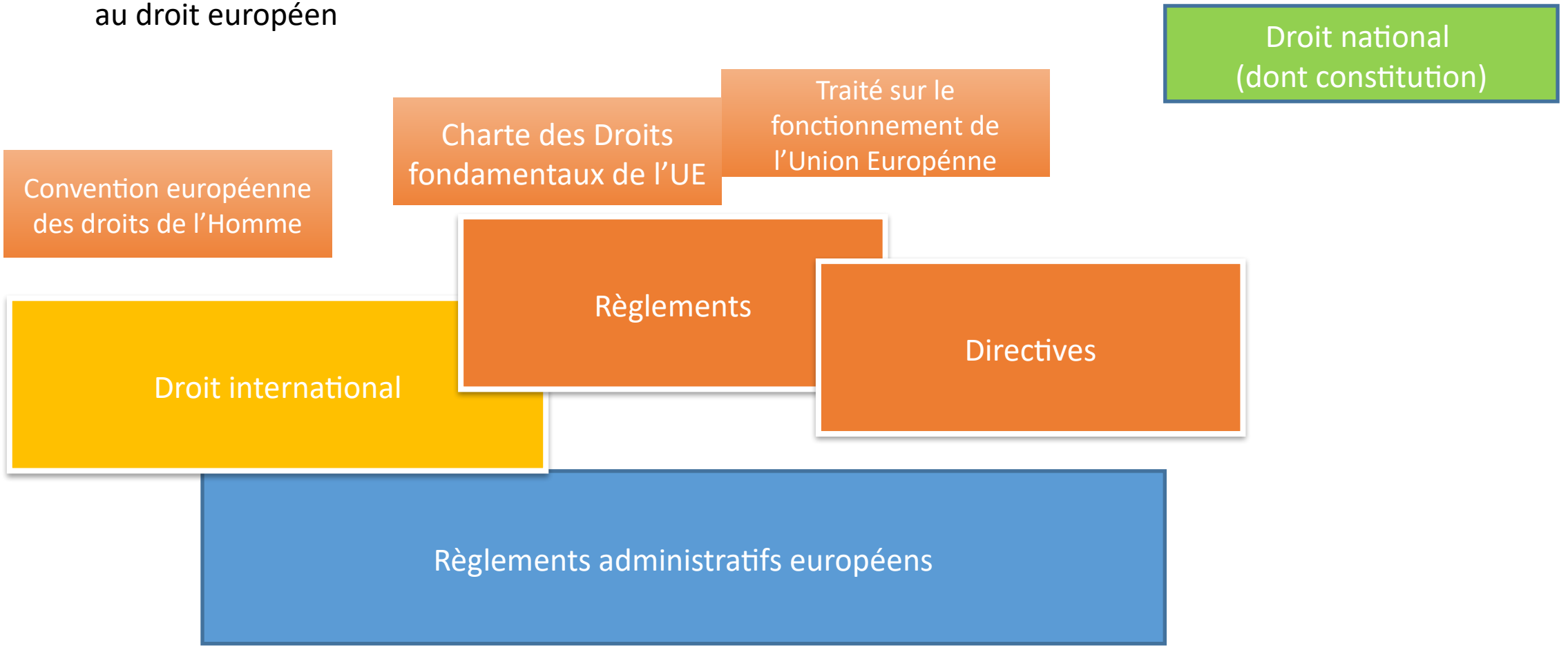
2. Un contexte géopolitique particulier : tension entre deux conceptions de l'Europe

Pyramide de Kelsen : hiérarchie du droit européen

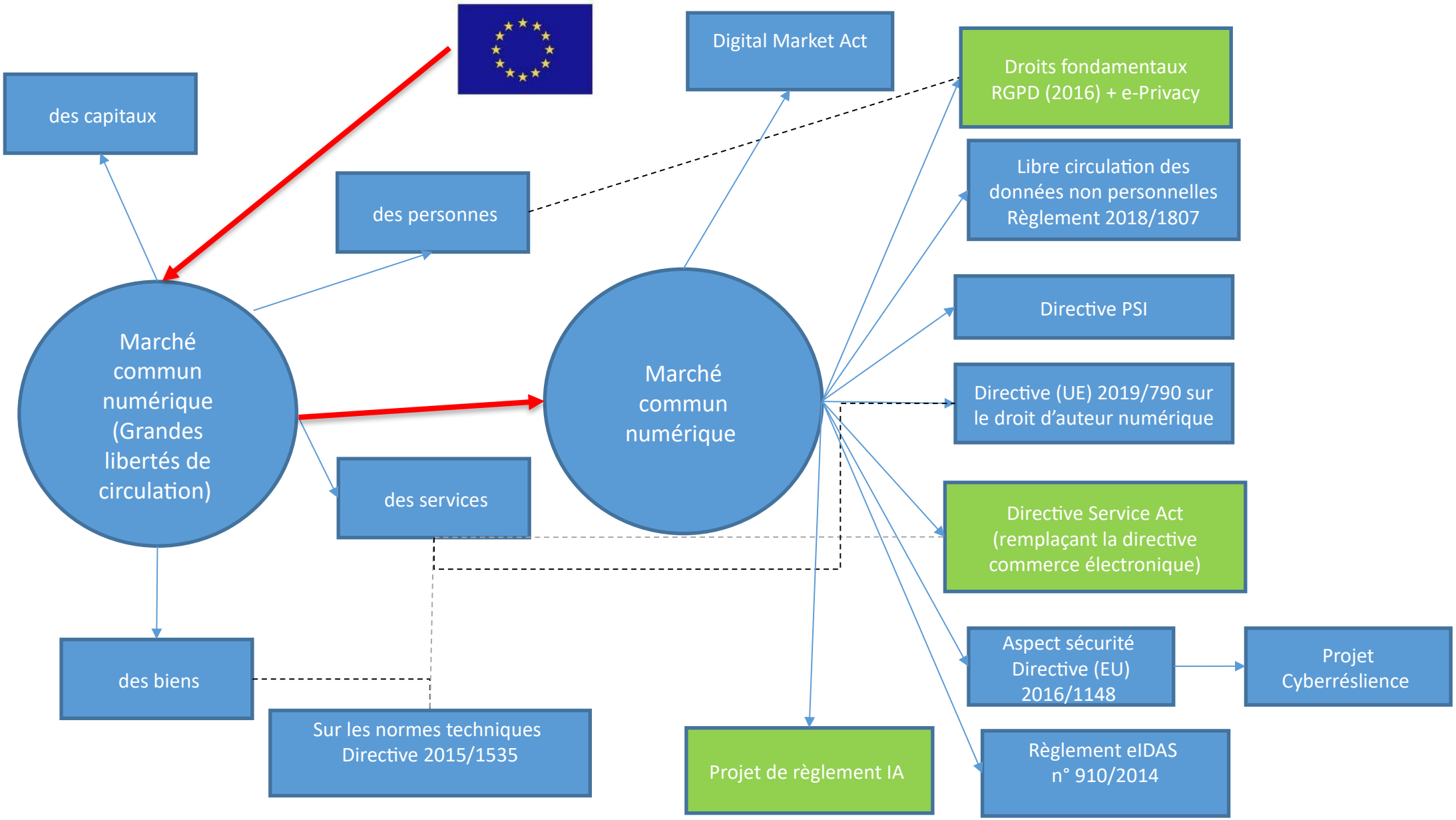


Pyramide de Kelsen version souverainiste : remise en cause de la hiérarchie des normes par certains pays

- arrêts obtenus par la Hongrie (CEDH Baka) et la Pologne (CEDH Dolińska-Ficek et Ozimek c. Pologne)
- Conseil d'Etat français sur la collecte des données de connexion
- invocation de plus en plus récurrente de la compétence pénale et de la sécurité intérieure pour se soustraire au droit européen



3. La volonté de construction d'une réglementation numérique européenne



3. La volonté de construction d'une réglementation numérique européenne

A. La protection (de l'industrie) européenne

Par des règlements européens de mise sur le marché

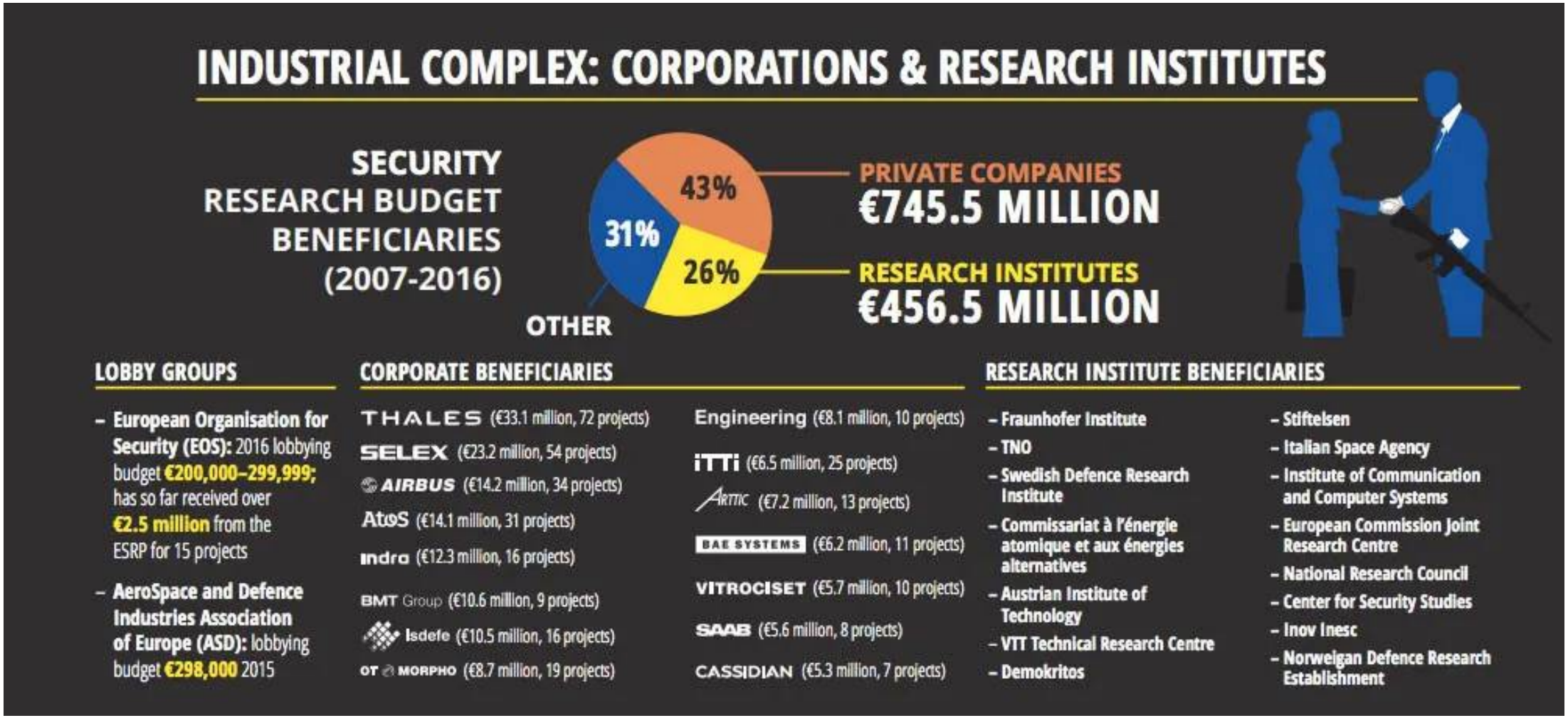
- Comble les lacunes du droit du commerce international où l'OMC négocie les règles
- Le numérique ne fait pas (directement) partie des règles du commerce international traditionnel

Comme soutien ou impulseur à des industries européennes

- Par les programmes de recherches « européens » (ex: Gaia X)

3. La volonté de construction d'une réglementation numérique européenne

B. Un secteur en plein essor: le capitalisme européen de la surveillance



4. L'AIA (Artificial Intelligence Act, Projet de règlement sur l'IA)

<u>Pourquoi l'AIA ?</u>

Absence de réglementation uniforme

- Sectorielle
- Entre Etats membres de l'Union européenne

Sur-médiatisation de l'intelligence artificielle

- Besoin de **confiance**
- Besoin d'une **réponse juridique**

En réaction, proposition d'un règlement par la Commission européenne

21 avril 2021, proposition établissant des règles harmonisées concernant l'intelligence artificielle ou « **AI Act** »

Objectif d'offrir **un cadre réglementaire harmonisé** dans l'Union européenne

- Economiquement utile car une règle pour tous
- Principe de reconnaissance mutuelle
- Permet d'assurer un niveau de protection des personnes

Le projet de règlement n'encadre pas toute l'IA

- Notion large de système d'intelligence artificielle
- Mais limité par *l'approche par les risques*

Définition de l'intelligence artificielle

par l'annexe 1 de l'AIA (*encore en cours d'élaboration*)

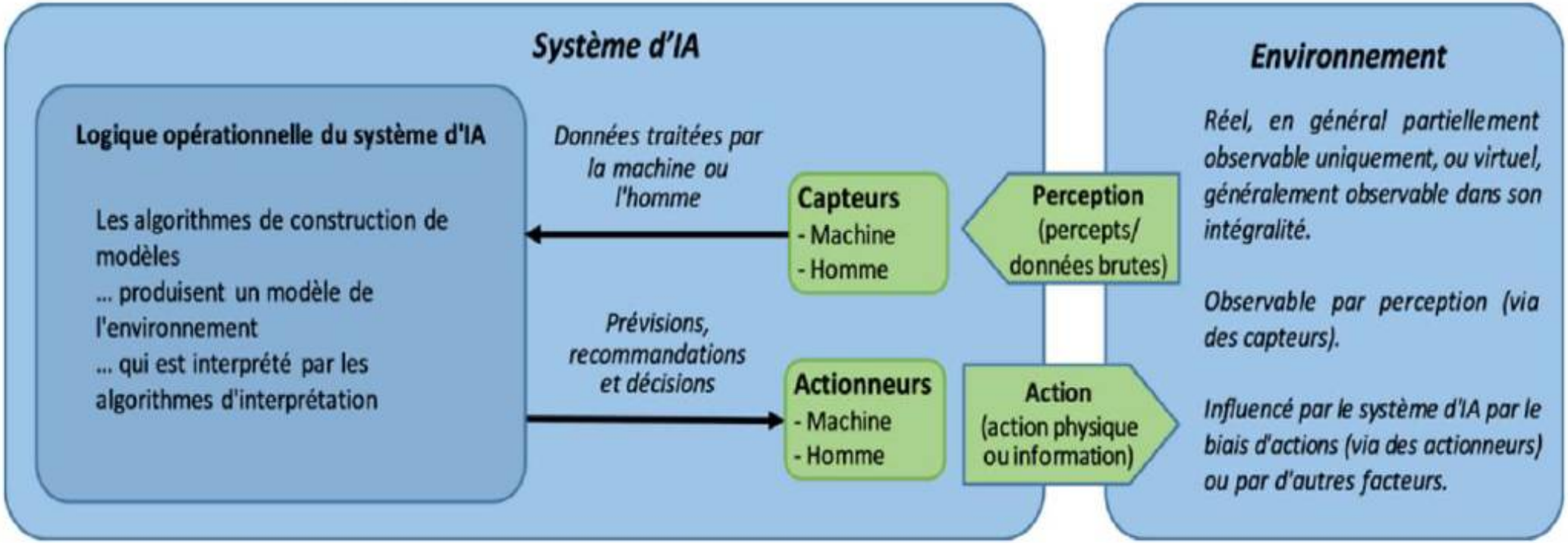
- Approches d'apprentissage automatique, y compris d'apprentissage supervisé, non supervisé et par renforcement, utilisant une grande variété de méthodes, y compris l'apprentissage profond
- Approches fondées sur la logique et les connaissances, y compris la représentation des connaissances, la programmation inductive (logique), les bases de connaissances, les moteurs d'inférence et de déduction, le raisonnement (symbolique) et les systèmes experts
- Approches statistiques, estimation bayésienne, méthodes de recherche et d'optimisation

par le Conseil d'Etat : il distingue si c'est un produit ou un service,

ou par le type de modèle utilisé

- IA apprentissage automatique
- Système expert
- Fonction générique
  - Reconnaissance d'image
  - Génération de texte
  - Prédictive

Vision conceptuelle d'un SIA (par le Conseil d'Etat)



Limites à l'application de l'Intelligence artificielle

- « Approche par les risques » avec trois niveaux de risque réglementés

Risque inacceptable : IA prohibées (art. 5)

Exemple : notation des citoyens, la reconnaissance faciale

Haut risque : IA encadrées (art. 6 à 51)

Exemple : véhicules agricoles et forestiers

Faible risque : IA soumises à des obligations de transparence (art. 52)

Exemple : *deep fake*

- L'exclusion du militaire est résolue par la non application de l'AIA
- Celle du maintien de l'ordre est en suspens

Cas d'interdiction d'utilisation de l'intelligence artificielle (d'après l'article 5 de l'AIA)
Les pratiques en matière d'intelligence artificielle suivantes sont interdites

L'utilisation de **systèmes d'identification biométrique à distance «en temps réel» dans des espaces accessibles au public à des fins répressives**, **sauf** si cette utilisation est strictement nécessaire selon l'un des objectifs suivants :
- la **recherche ciblée de victimes potentielles spécifiques de la criminalité**, notamment d'enfants disparus;
- la **prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique des personnes physiques ou la prévention d'une attaque terroriste** ;
- la **détection, la localisation, l'identification ou les poursuites à l'encontre de l'auteur ou du suspect d'une infraction pénale** (…) punissable dans l'État membre concerné d'une peine ou d'une mesure de sûreté privatives de liberté d'une **durée maximale d'au moins trois ans**, déterminées par le droit de cet État membre.

Cette utilisation **tient compte de la nature de la situation** donnant lieu à un éventuel recours au système, en particulier **la gravité, la probabilité et l'ampleur du préjudice causé en l'absence d'utilisation du système**;

En outre, cette utilisation doit respecter **les garanties et conditions nécessaires et proportionnées** en ce qui concerne cette utilisation, notamment **eu égard aux limitations temporelles, géographiques et relatives aux personnes**.

Chaque utilisation est subordonnée à une **autorisation préalable octroyée par une autorité judiciaire ou une autorité administrative indépendante** de l'État membre dans lequel cette utilisation doit avoir lieu, délivrée sur demande motivée et conformément aux règles détaillées du droit national. Toutefois, dans une situation d'urgence dûment justifiée, il est possible de commencer à utiliser le système sans autorisation et de ne demander l'autorisation qu'en cours d'utilisation ou lorsque celle-ci a pris fin.
L'autorité judiciaire ou administrative compétente n'accorde l'autorisation que si elle estime, sur la base d'éléments objectifs ou d'indications claires qui lui sont présentés, que **l'utilisation du système d'identification biométrique à distance «en temps réel»** en cause **est nécessaire et proportionnée à la réalisation de l'un des objectifs énumérés**, tels qu'indiqués dans la demande.
Un État membre peut décider de prévoir la possibilité d'autoriser totalement ou partiellement l'utilisation de ces systèmes dans les limites et les conditions définies.

Position des acteurs politiques

- La liste des systèmes d'IA dont l'UE interdira l'utilisation sur son sol pourrait elle aussi s'allonger, malgré des désaccords plus radicaux encore à cet égard. Les négociations s'annoncent particulièrement ardues sur l'identification biométrique.
- La Commission proposait d'interdire l'utilisation de systèmes d'identification biométrique à distance « en temps réel dans des espaces accessibles au public à des fins répressives » sauf lorsque ces systèmes sont utilisés pour rechercher des victimes, « prévenir une menace spécifique, substantielle et imminente pour la vie ou la sécurité » des citoyens, identifier ou poursuivre l'auteur d'une infraction pénale.
- Le S&D, les Verts et la Gauche plaident au contraire pour une interdiction pure et simple de tous les systèmes d'identification biométrique utilisés à distance, dans les espaces publics comme privés, en ligne et hors ligne.
- Les rapporteurs Renew sont, eux, favorables à l'interdiction des systèmes d'identification biométrique lorsqu'ils sont utilisés à distance « en temps réel » dans les espaces accessibles au public, et ne tolèrent pas d'exceptions.
- Le PPE avance pour sa part une position en phase avec celle de la Commission, soutient les exceptions proposées et maintient que l'utilisation de ces systèmes « a posteriori » devrait simplement être considérée comme « à haut risque ».
- Comme les corapporteurs, les Verts et La Gauche voudraient également interdire la « police prédictive » – que le PPE préférerait, lui, maintenir dans la catégorie « haut risque ».
- Le S&D, les Verts, La Gauche, ainsi **qu'ID et les CRE veulent aussi bannir les systèmes permettant de détecter l'état émotionnel, la fiabilité des personnes ainsi que diverses caractéristiques physiques**.
- Plusieurs groupes à gauche prônent, en outre, l'interdiction des systèmes dédiés à la gestion de la migration et à l'examen des demandes d'asile.

5. Flou juridique entre les polices judiciaire (qui se réfère au RGPD) et administrative (… au LED)

- à quel moment une donnée « personnelle » administrative collectée dans le cadre d'une action de police administrative devient une donnée « personnelle » judiciaire utilisée à titre probatoire
- cela pose la question de la collecte de données généralisées

Plusieurs arrêts ont jugé de la capture des données indifférenciées : Arrêt LQDN (CJUE), surtout Procatuur (CJUE),
Big Brother (CEDH), Centrum (CEDH).
La CJUE précise que le droit de l'Union ne s'oppose pas à la législation d'un État membre prévoyant une conservation ciblée des données aux fins de la :

- lutte contre la criminalité grave
- prévention des menaces graves contre la sécurité publique.

Elle évoque ainsi **diverses hypothèses** dans lesquelles une telle conservation peut s'envisager, à savoir, lorsqu'elle est :

ciblée et délimitée « *des données relatives au trafic et des données de localisation* » *:*

- sur la base d'éléments objectifs et non discriminatoires,
- en fonction de catégories de personnes concernées ou
- au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;

généralisée et indifférenciée des :

- « *adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire* » ;
- « *données relatives à l'identité civile des utilisateurs de moyens de communications électroniques* » ;

réalisée dans le cadre d'une injonction enjoignant les opérateurs à procéder :

« *pour une durée déterminée, à la conservation rapide (quick freeze) des données relatives au trafic et des données de localisation* ».

A la condition toutefois que ces mesures assurent, « *par des règles claires et précises, que la conservation des données en cause est subordonnée au* ***respect des conditions matérielles et procédurales*** *y afférentes et que les personnes concernées disposent de* ***garanties effectives contre les risques d'abus*** »

6. La reconnaissance faciale
- Définition selon les processus

- Technique dite de vision par l'ordinateur qui analyse des images pour identifier et de caractériser des personnes à partir de leurs caractéristiques physiques (formes, protection)
- Le CEPD définit les données biométriques correspondants aux images permettant l'identification et la caractérisation des personnes comme **incluant tout traitement automatique permettre de quantifier des caractéristiques physiques, physiologiques ou comportements (empreintes digitales, structure de l'iris, la voix, etc…**).
- Ces techniques reposent sur un gabarit (une photographie) dont il est possible d'extraire une représentation numérique des éléments caractéstiques de la personne.
- Un modèle biométrique est une représentation numérique des caractéristiques uniques qui ont été extraites d'un échantillon biométrique et qui peuvent être stockées dans une base de données biométriques. Ce modèle est censé être unique et spécifique à chaque personne et il est, en principe, permanent dans le temps.
- Dans la phase de reconnaissance, le dispositif compare ce gabarit à d'autres gabarits préalablement produits ou calculés directement à partir d'échantillons biométriques tels que des visages trouvés sur une image, une photo ou une vidéo.
- " La reconnaissance faciale " est donc un **processus en deux étapes : la collecte de l'image du visage et sa transformation en gabarit, puis la reconnaissance de ce visage par comparaison du gabarit correspondant avec un ou plusieurs autres gabarits.**

- Définition selon les fonctions

Comme tout processus biométrique, la reconnaissance faciale peut remplir deux fonctions distinctes :

- **l'authentification d'une personne, visant à vérifier qu'une personne est bien celle qu'elle prétend être**. Dans ce cas, le système va comparer un modèle ou un échantillon biométrique préenregistré (par exemple, stocké sur une carte à puce ou un passeport biométrique) avec un seul visage, comme celui d'une personne se présentant à un point de contrôle, afin de vérifier s'il s'agit d'une seule et même personne. Cette fonctionnalité repose donc sur la comparaison de deux modèles.
- **l'identification d'une personne, visant à retrouver une personne parmi un groupe d'individus, dans une zone spécifique, une image ou une base de données**. Dans ce cas, le système doit effectuer un test sur chaque visage capturé pour générer un modèle biométrique et vérifier s'il correspond à une personne connue du système. Cette fonctionnalité repose donc sur la comparaison d'un gabarit avec une base de données de gabarits ou d'échantillons. C'est ce qu'on appelle également l'identification 1 à plusieurs.

De nombreux contextes différents :

- dans la relation personnelle entre un utilisateur et un service (accès à une application),
- pour l'accès à un lieu spécifique (filtrage physique), ou sans limitation particulière dans l'espace public (reconnaissance faciale en direct).

Elle peut s'appliquer à tout type de personne concernée : un client d'un service, un employé, un simple badaud, une personne recherchée ou impliquée dans une procédure judiciaire ou administrative.

Exemples d'identification par reconnaissance faciale

- L'identification peut être appliquée de nombreuses manières, encore plus diverses. Il s'agit notamment des utilisations énumérées ci-dessous, actuellement observées, expérimentées ou prévues dans l'UE.
- recherche, dans une base de données de photographies, de l'identité d'une personne non identifiée (victime, suspect, etc.).
- suivi des déplacements d'une personne dans l'espace public. Son visage est comparé aux gabarits biométriques des personnes circulant ou ayant circulé dans la zone surveillée, par exemple lorsqu'un bagage est oublié ou après qu'un crime a été commis.
- la reconstitution du parcours d'une personne et de ses interactions ultérieures avec d'autres personnes, par une comparaison différée des mêmes éléments en vue d'identifier ses contacts par exemple.
- l'identification biométrique à distance des personnes recherchées dans les espaces publics. Tous les visages captés en direct par les caméras de vidéo-protection sont croisés, en temps réel, avec une base de données détenue par les forces de sécurité.

7. Les justifications d'une ingérence étatique pour le traitement des étrangers

Le lien de la réglementation numérique européenne avec les ressortissants étrangers semble ténu, mais il est pourtant existant :

l'élaboration des frontières extérieures à l'UE crée un formalisme permettant le respect des grandes libertés sur le marché intérieur (Règlement Itar).

MAIS la question migratoire reste de l'apanage des Etats

Défaut de Citoyenneté : suspicion de terrorisme ou d'espionnage

Acceptabilité sociale:

- exemple utilisation des plateformes de rdv à la préfecture pour renouvellement des visas versus les problèmes de passeports
- Sert de fondement narratif pour les pouvoirs publics
  (ok facebook pourquoi pas pour la préfecture ?)

A. Les étrangers comme béta-testeurs

- *Exemple : application limitée du RGPD pour les étrangers lors du projet Alicem*

- Analyse Alicem sous le sceau du RGPD avant de le rattacher au CESEDA : « la Commission [CNIL] rappelle qu'il a pour finalité principale de garantir le droit au séjour des ressortissants étrangers **en situation régulière et de lutter contre l'entrée et le séjour irréguliers en France des ressortissants étrangers**. Ce traitement constitue ainsi le fichier principal de gestion administrative des étrangers en France et permet notamment la gestion, par les préfectures, des dossiers de ressortissants étrangers, la fabrication des titres de séjour et **la gestion des mesures d'éloignement.** »

- Or ces mesures relèvent du droit « pénal » administratif : cf Règlement (UE) 2018/1240 du Parlement européen et Conseil du 12 septembre 2018 (création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

- **Donc soumission progressive au caractère « pénal » et donc soumission au LED**

- **Compétence des Etats pour l'accueil des ressortissants étrangers :** même si limitation par la jurisprudence de la CJUE qui a donné de nombreux droits aux familles de ressortissants d'Etats tiers en droit européen.

Mais qu'a-t-on vu surtout d'Alicem ? Des failles partout **:**

- Dans les résultats

*Taux de **faux refus** (niveau faible requis pour garantir l'adhésion des utilisateurs et la bonne utilisation : moins de 20%.*
*Taux de **fausse acceptation** (en cas d'utilisation conforme ou d'une tentative de fraude) suffisamment bas pour garantir une sécurité optimale et limiter le risque d'usurpation : moins de 0,9%.*

- Dans l'UX :

Absence notoire de niveaux de lecture ;
Mauvaise architecture de l'information (rapport texte / action parfois difficile à identifier) amplifiée par un manque de contraste entre les types d'éléments ; Ce manque de structuration entraine des déficiences en termes d'accessibilité.
La mauvaise utilisation des composants Material Design [du nom donné par Google à un ensemble de règles de design censées améliorer l'expérience utilisateur, ndlr] *est un frein à la prise en main rapide de l'utilisateur et pourrait causer des problèmes de compatibilité sur certains téléphones ou versions d'Android (parc très hétéroclite).*

- Enrôlement foireux

Qu’est ce que cela change concrètement pour les étrangers ?

Beaucoup de choses :

Le recours au fondement légal c’est-à-dire par le vote des députés d’une loi

Donc moins de protections effectives (même si le CC est censé protégé tout le monde)

- Mais principe de discrimination pour les étrangers
- La distinction structurelle entre « européens » et « ressortissants d’Etats tiers » : « Public vulnérable » entraînant une sorte de discrimination par affinité
- Avec un réel risque de chilling effect (ce qui veut dire le non exercice des droits de peur d’être sanctionné(e))

B. Des zones sensibles à protéger

Définition des zones sensibles à protéger :

Décision du Conseil Constitutionnel, Loi relative à la responsabilité pénale et à la sécurité intérieure (2021-834)

Autorisation des caméras embarquées si et seulement si :

- assurent la sécurité des interventions de ces services (càd commission d'agressions sur les agents impliqués dans une opération de police ou de secours) pour l'envoi éventuel de renforts
- l'enregistrement est déclenché que lorsque se produit ou est susceptible de se produire un incident, eu égard aux circonstances de l'intervention ou au comportement des personnes concernées et limité à cette intervention.
- si uniquement des images captés sur des lieux publics.

8. Par rapport au cas présenté au départ : « *reconnaissance faciale appliquée à des personnes étrangères dans les gares* »

Cela renvoie au projet de délibération présenté par Laurent Waukiez le 19 juillet 2021 au Conseil régional de la région Auvergne-Rhône-Alpes, en quatre points :
- « *accompagner, [dans les trains régionaux et les gares] à titre expérimental, un premier dispositif de reconnaissance faciale, uniquement accessible aux autorités compétentes* » ;
- « *déployer la **vidéoprotection à l'intérieur des cars scolaires** et interurbains* » ;
- « *poursuivre l'équipement en **caméras de vidéoprotection en temps réel** des trains régionaux* » ;
- « *renforcer le bouclier "vidéoprotection" avec 10 000 caméras supplémentaires et en l'étendant à la vidéoprotection intelligente ainsi qu'à l'expérimentation de systèmes innovants (exemple : la technologie biométrique…)* ».

D'après les pistes juridiques présentées, la principale se situerait (si le règlement sur l'intelligence artificielle est adopté), en référence à son **article 5 (usages prohibés de l'IA)**, dans la **contestation de l'utilisation de ce système comme n'étant ni nécessaire ni proportionné à la réalisation de ses objectifs**.