

L'utilisation de l'IA à des fins de prévention et de poursuite: analyse des risques et du cadre réglementaire

Prof. Vanessa Franssen

CAS Droit et intelligence artificielle
Module 8
Université de Neuchâtel
Institut Catholique de Paris
25 avril 2026



Plan



1. Introduction

- Définition et types d'IA
- Délimitation: « à des fins de prévention et de poursuite »
- Plus-value de l'IA

2. Détection

3. Prédiction (afin de prévenir)

4. Enquêtes et poursuites

5. Conclusions

1. Introduction



1. Introduction

- Qu'est-ce que l'IA?

- Selon ChatGPT (“*mise en abyme*”)
 - AI “refers to the ability of a machine or computer program to perform **tasks that would typically require human intelligence**. These tasks include things like **learning from data**, reasoning, **problem-solving**, understanding natural language, and even recognizing patterns or making decisions.”
 - “In essence, AI is about creating systems that can **simulate human-like intelligence** in various ways!”

<https://i.pinimg.com/736x/02/ec/bf/02ecbf3dd022dff6571d81791c56359a.jpg>





1. Introduction

• Qu'est-ce que l'IA? (suite)

- Selon ChatGPT (suite)
 - Deux types
 - **Systèmes d'IA spécifiques (« narrow AI ») ou IA faible**
 - « is specialized for specific tasks—like a chatbot, a recommendation system, or self-driving cars. It excels in the task it's trained for but lacks general intelligence across a wide range of activities. »
 - **Systèmes d'IA généraux (« general AI ») ou IA forte**
 - « is a more theoretical concept where machines could perform any cognitive task that a human can. It would have the ability to think, understand, learn, and apply knowledge in various areas, similar to how humans do. »
 - Quelques sous-domaines
 - **Apprentissage automatique (« machine learning »)**, où les algorithmes apprennent par eux-mêmes)
 - ... « **natural language processing** » (NLP) , ex. technologie utilisée pour les chatbots
 - « **computer vision** », où la machine interprète des données visuelles et prend des décisions sur la base de ces données



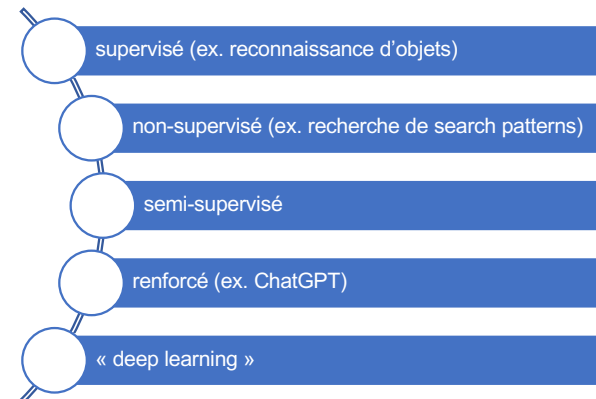
1. Introduction

• Qu'est-ce que l'IA? (suite)

- D'autres distinctions bien connues < littérature

Ancienne
distinction

- « **Expert systems** » ou systèmes basés sur les règles (« top-down »)
 - Le système reproduit le raisonnement humain
 - Le développeur (pré)définit les tâches et les modalités d'exécution
 - -> tâches bien définies
- « **Data-based systems** » ou systèmes basés sur l'apprentissage (« bottom-up ») -> apprentissage automatique (« machine learning »)
 - Le système détectera lui-même des modèles et apprend par lui-même
 - Plus opaque -> interprétabilité? (*infra*) (« white box AI »)





1. Introduction

• Qu'est-ce que l'IA? (suite)

- D'autres distinctions bien connues < littérature

Plus
récentes

- **IA générative**

- Création de contenu
- Ex. images, vidéos, ... -> problématique des deepfakes, = mode opératoire de criminels (*infra*)

- **IA agentique**

- Basée sur l'IA generative et l'utilisation de grands modèles de langage ("LLM")
- « un système d'intelligence artificielle capable d'atteindre un objectif précis avec une **supervision limitée**. Il se compose d'agents IA, de modèles de machine learning capables **d'imiter la prise de décision humaine** pour résoudre des problèmes **en temps réel**. Dans un système multi-agent, chaque agent exécute une tâche spécifique et leurs actions sont coordonnées grâce à l'orchestration de l'IA »
- « fait preuve d'**autonomie**, d'un comportement orienté objectif et d'adaptabilité »
- « capacité à agir de manière **indépendante et ciblée** » (IBM, 24 avril 2026)
- An "advanced form of AI focused on autonomous decision-making and action. Unlike traditional AI, which primarily responds to commands or analyzes data, agentic AI can **set goals, plan, and execute** tasks with **minimal human intervention**. This emerging technology has the potential to **revolutionize** various industries by automating complex processes and optimizing workflows ». (Google Cloud, 27 Jan. 2026)

>< modèles IA
traditionnels

- ...

Cadre
réglementaire
(*infra*) en phase
avec la
technologie?



1. Introduction

• Qu'est-ce que l'IA? (suite)

• Au sens juridique

- Au niveau de l'**UE**

- Art. 3, § 1 règlement sur l'IA (« AI Act »)(2024)

Définition axée sur l'autonomie et les résultats produits, basée sur une approche par les risques

- 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 virtuel »

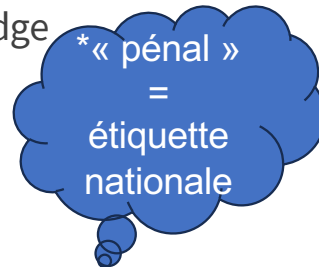
- Cf. définition du **Conseil de l'Europe**: art. 2 Convention cadre sur l'IA (2024)
- Cf. définition de l'**OCDE**



1. Introduction

• « A des fins de prévention (, de détection) et de poursuite »

- Anglais: « for law enforcement purposes »
 - Définition large: “the activity of making certain that the laws of an area are obeyed” (Cambridge Dictionary)
 - Définition plus stricte: justice pénale (ex. Wikipedia)
- Expression utilisée en droit de l’UE - exemples
 - Directive “Police” (UE) 2016/680 = pendant “justice” du RGPD
 - « (...) autorités compétentes à des fins de **prévention** et de **détection** des infractions **pénales***, d’enquêtes et de **poursuites** en la matière ou d’exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces » (art. 1, § 1^{er})
 - = autorités répressives
 - Directive e-privacy 2002/58/CE
 - « assurer la prévention, la recherche, la détection et la poursuite d’infractions **pénales*** » (art. 15, § 1^{er})
 - Directive conservation des données 2006/24/CE (invalidé par la CJUE en 2014)
 - Jurisprudence de la Cour de justice de l’Union européenne (CJUE) – JP sur la conservation de données électroniques
 - « aux fins de lutte contre la criminalité (grave) »



Droit
pénal,
enquêtes
pénales*

1. Introduction

- « **A des fins de prévention (, de détection) et de poursuite** » (suite)
- Mais le cas échéant aussi certains **stades antérieurs...** (prévention)
 - Directive « Police »: « y compris la protection contre les menaces pour la **sécurité publique** et la **prévention** de telles menaces »
 - CJUE: « la **prévention** des **menaces ou atteintes graves** contre la **sécurité publique** »



Délimitation?

À distinguer des renseignements



1. Introduction

• « A des fins de prévention (, de détection) et de poursuite » (suite)

- Et *quid* du **droit administratif « punitif »**?
 - **Pas** de du droit pénal au sens strict
 - = du « quasi-pénal »
 - Mais du “pénal” au sens des articles 6-7 CEDH
 - -> Application des **droits fondamentaux** en matière pénale
 - Ex. procès équitable (juge indépendant et impartial), présomption d’innocence, droits de la défense...
 - Ex. droit de la concurrence, marchés financiers, droit fiscal, droit du travail/social, droit de la migration, droit douanier...

V. Franssen, « La notion ‘pénale’: mot magique ou critère trompeur ? Réflexions sur les distinctions entre le droit pénal et le droit quasi pénal », in D. Brach-Thiel (dir.), *Existe-t-il un seul non bis in idem aujourd’hui?*, Paris, L’Harmattan, 2017, pp. 57-91.

V. Franssen et C. Harding (dir.), *Criminal and Quasi-criminal Enforcement Mechanisms in Europe: Origins, Concepts, Future*, Oxford, Hart/Bloomsbury Publishing, 2022, 430p.



1. Introduction

- « A des fins de prévention (, de détection) et de poursuite » (suite)

- Ce cours-ci

- Droit pénal (au sens strict) ➔ infractions pénales

- Mais aussi droit administratif punitif ➔ infractions/contraventions administratives

- Et les activités des autorités compétentes en la matière

- **Autorités publiques**

- Peut-être aussi des **acteurs privés**...?! (cf. définition d'autorités compétentes par la Directive « Police »)

- Rôle du secteur privé dans une société démocratique?
 - Collaboration avec les autorités publiques?



Questions
fondamentales
!

1. Introduction

- **Plus-value de l'IA ...**

- **De façon générale**

- Vitesse
 - Intelligence “collective”
 - Intelligence qualitative (?)

- **Dans le domaine de la justice pénale?**



1. Introduction

- **Plus-value de l'IA pour le domaine de la justice pénale?**

- Selon Chat GPT
 - “AI has the potential to significantly reshape law enforcement in various ways, both positively and with some challenges. Here's how AI could impact the field:
 - **1. Predictive Policing**
 - AI can analyze large sets of data (crime patterns, trends, geography, time of day, etc.) to predict where crimes are likely to occur or even who may be involved. This can help law enforcement allocate resources more effectively, but it also raises concerns about privacy and the risk of over-policing certain communities.
 - **2. Facial Recognition and Surveillance**
 - AI-powered facial recognition technology can be used to identify suspects or persons of interest from public or private video footage. It can speed up investigations, but its use is controversial, as it might lead to privacy violations and potential bias in identifying individuals from minority groups. (...)”



Bonne
réponse?

1. Introduction

• Plus-value de l'IA pour le domaine de la justice pénale? (suite)

- Selon Chat GPT (suite)
 - **“3. Automation of Routine Tasks**
 - AI can help streamline administrative and routine tasks, such as processing evidence, filling out reports, or managing databases. This can save officers time and allow them to focus more on on-the-ground policing.
 - **4. AI in Crime Detection**
 - AI algorithms can be used to analyze digital evidence, such as emails, social media posts, or other communications, to detect criminal activity (e.g., human trafficking, online fraud, cybercrime). It can also help identify emerging threats and illicit behavior.
 - **5. Enhanced Forensic Analysis**
 - AI tools can assist in processing and analyzing forensic data (such as DNA, fingerprints, or digital forensics). Machine learning algorithms can identify patterns or link evidence in ways that human analysts might miss, leading to faster and more accurate conclusions.
 - **6. Automated Drones and Robots**
 - AI-powered drones and robots could be used for surveillance, search and rescue, or even disarming dangerous situations. Drones, for example, could help in monitoring large crowds or gathering real-time intelligence from hard-to-reach areas.(...)” -> e.g. Olympics in Paris (2024)



1. Introduction

• Plus-value de l'IA pour le domaine de la justice pénale? (suite)

- Selon Chat GPT (suite)
 - “**7. Bias and Accountability Issues**
 - (...)
 - **8. AI-Assisted Decision Making**
 - AI can support law enforcement officers in making more informed decisions. For example, in high-stakes situations, AI could help officers assess risks based on historical data, previous interactions, and other relevant factors.
 - **9. Cybercrime and Threat Detection**
 - AI can help detect and respond to cybercrimes more effectively. It can analyze huge amounts of data to recognize patterns and behaviors indicative of cybercriminal activities, such as hacking attempts, identity theft, or online terrorism.
 - **10. Real-Time Crime Monitoring**
 - AI can power smart city infrastructure, like surveillance cameras, traffic sensors, and other IoT devices, to create a real-time crime monitoring system. By analyzing data from various sources, AI can alert law enforcement to incidents as they happen.
- Challenges (...)
- Ultimately, while AI can enhance efficiency and capabilities within law enforcement, it's essential to balance its use with ethical considerations and safeguards to prevent misuse.”

Fondé sur
les preuves



Réflexion
humaine,
basée sur
les valeurs

1. Introduction

• Plus-value de l'IA pour le domaine de la justice pénale? (suite)

Éléments clés

- **Détection** (Partie 2)
- **Prédiction** (de faits) (Partie 3)
 - Pour prévenir, intervenir, agir en temps utile
- **Enquêtes et poursuites** (Partie 4)
- Aide dans la **prise de décision**
 - Basée sur les preuves? (“evidence-based”)
 - Mieux acceptée?
- **Exécution** des peines?

Pas abordé dans
ce cours



2. Détection



2. Détection

• Exemples

- Détection de fraude fiscale

- Ex. Connect (UK), Oasis (BE), Galaxie (FR)...
- Data mining & data matching
 - Données en possession des autorités
 - « open source »
 - Cadre juridique spécifique (cf. RGPD)
 - Nouvelle loi belge fort discutée: loi du 18 déc. 2025 portant dispositions diverses, *M.B.*, 30 déc. 2025

- Suspicion -> enquête

- = base de beaucoup d'enquêtes!

Autorités
publiques

Obligation de
fournir des
documents – droit
au silence?



2. Détection

• Exemples (suite)

- Détection de fraude sociale
 - Ex. allocations familiales/sociales aux Pays-Bas, système « System Risk Indication algorithm » (SyRi)
 - Indication de risque
 - Scandale...faux positifs -> impact énorme
 - [District Court of the Hague of 5 February 2020](#) (§§ 6.45 et s.): violation de l'art. 8 CEDH, manque de transparence (quel modèle de risques, quels indicateurs?)

Autorités publiques



Open Global Rights

Analyzing the present and future of human rights

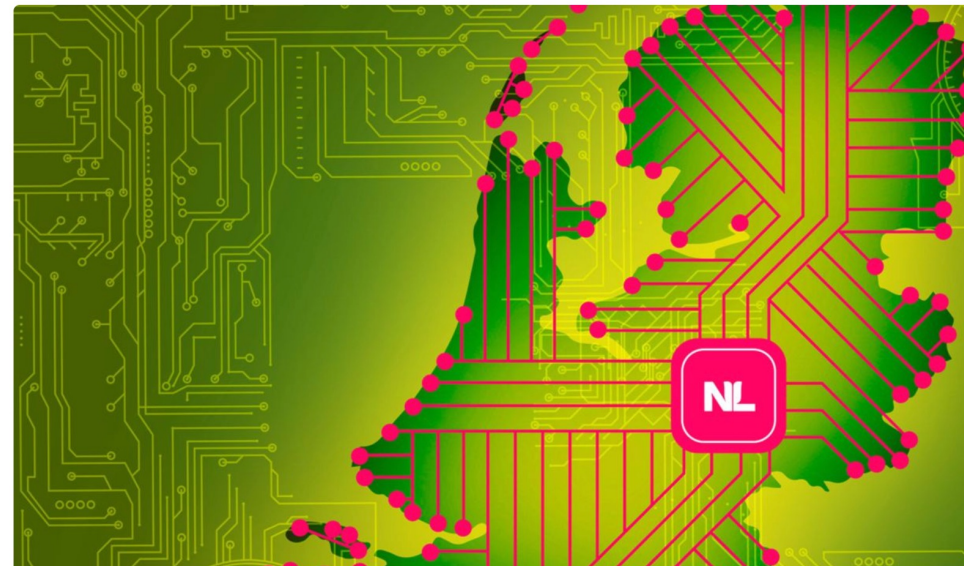
Articles Sections ▾ Series ▾ Multimedia ▾ At

March 19, 2020

Aux Pays-Bas, une décision judiciaire historique sur les États-providences numériques et les droits humains

Aux Pays-Bas, une décision judiciaire historique montre que la technologie utilisée par les pouvoirs publics pour lutter plus « efficacement » contre les fraudes commises contre l'État providence peut engendrer de l'exclusion injustifiée, de la discrimination et de la stigmatisation.

By Christiaan van Veen



<https://www.openglobalrights.org/landmark-judgment-from-netherlands-on-digital-welfare-states/?lang=French>

2. Détection

• Exemples (suite)

- Détection de collusions (droit de la concurrence)
- Détection de manipulation des marchés
 - Ex. FSMA en Belgique utilise des outils d'IA)
- Détection de risques en matière douanière -> cibler des inspections
 - -> réforme du CCU et création de l'Autorité douanière européenne (Lille)
- Etc.

Autorités
publiques



STANFORD
COMPUTATIONAL
ANTITRUST



ARTICLE

Cartel Screening and Machine Learning

Joseph E. Harrington, Jr.* & David Imhof**

Abstract. This paper discusses a growing tool of interest for cartel detection: examining market data for evidence of collusion, or what is referred to as cartel screening. Screening identifies collusive patterns in firm conduct such as prices and bids. The first half of the paper describes what to look for in the data, more specifically it features collusive markers, structural breaks, and anomalies. A collusive marker is a pattern in the data more consistent with collusion than competition. A structural break is an abrupt change in the data-generating process that could be due to cartel birth, death, or disruption. An anomaly is a pattern in

2. Détection

Autorités
publiques

• Risques

- Droit au respect de la vie privée
- Protection des données à caractère personnel
- Droit à la non-discrimination
- Droit au procès équitable (+ droits de défense)
 - Biais?
 - -> juge indépendant et impartial
 - Accès...?
 - -> fiabilité de la preuve, égalité des armes
 - Transparence...?
 - -> obligation de motivation, erreurs judiciaires, droit d'appel
- ...



Échange & accès
de données entre
autorités?

2. Détection

Autorités
publiques



- Cadre juridique

- RGPD + législations spéciales

Entrée en
vigueur
progressive

- AI Act

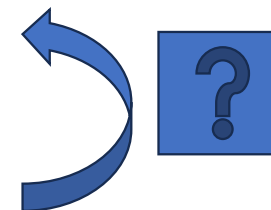
- **Approche par les risques**
- Pratiques interdites
 - Ex. « social scoring », évaluation et classification de personnes physiques (art. 5, § 1^{er}, c)
- Point 48 du préambule
 - « L'ampleur de **l'incidence négative** du système d'IA sur les **droits fondamentaux** protégés par la Charte est un critère particulièrement pertinent lorsqu'il s'agit de classer un système d'IA en tant que **système à haut risque**. »
- Si système à haut risque, plus d'obligations légales!
 - Quels systèmes? Art. 6 AI Act + annexe III
- *Pas un système à haut risque(?!): systèmes d'IA utilisées à des fins de détection de fraude financière (annexe III, point 5, b))*

Systèmes interdits (art. 5) (mais exceptions)

Systèmes à haut risque (art. 6) (mais exceptions)

« certains systèmes », risque limité (art. 50)

Systèmes d'IA à usage général, risque systémique



2. Détection

Council of the EU | Press release | 13 March 2026 12:33

Council agrees position to streamline rules on Artificial Intelligence

Today the Council agreed its position on the proposal to streamline certain rules regarding **artificial intelligence (AI)**.

The proposal forms part of the so-called “**Omnibus VII**” legislative package in the EU’s **simplification** agenda. The package includes proposals for two regulations aiming to simplify the EU’s digital legislative framework and the implementation of harmonised rules on AI.



Streamlining the AI rules is essential for ensuring the EU’s digital sovereignty. As presidency, we worked on this proposal with urgency, reaching a swift agreement to facilitate the timely application of the AI act. The proposal will bring greater legal certainty, make the rules more proportionate and ensure more harmonised implementation across member states. We are ready to work with our co-

- Report de l’entrée en vigueur de certaines règles
- Nouvelle pratique interdite (*infra*)
- Plus d’orientations à fournir par la Commission européenne aux opérateurs économiques – systèmes à haut risque
- Clarification du rôle du Bureau de l’IA (en lien avec art. 50 AI Act)

<https://www.consilium.europa.eu/en/press/press-releases/2026/03/13/council-agrees-position-to-streamline-rules-on-artificial-intelligence/>



2. Détection

Acteurs privés



• Exemple 1

- Détection de transactions financières irrégulières (« obligation AML »)
 - Lutte contre le **blanchiment d'argent (et le financement du terrorisme)**
 - Cadre légal national/européen/international + rôle du GAFI
 - Prévention ou détection?
 - Utilisation de cryptomonnaies/monnaies virtuelles
 - Par les entités/personnes assujetties à la législation anti-blanchiment
 - De + en + nombreuses!
 - Risque pénal pour ces personnes (participation punissable...)
 - Coopération avec les autorités policières/judiciaires

S. Vandeweerd et V. Franssen, « Le blanchiment de capitaux à l'ère des cryptomonnaies », in A. Vandenbulke (ed.), *Les aspects juridiques de la blockchain et de ses applications*, Vol. 2, Anthemis, 2024, pp. 207-259.

2. Détection

Acteurs privés



- Exemple 2

- Détection de **contenu illégal en ligne**
 - Risques
 - Droit au respect de la vie privée (art. 8 CEDH et art. 7 Charte des droits fondamentaux de l'UE)
 - Liberté d'expression (art. 10 CEDH et art. 11 Charte)
 - Cadre juridique
 - Définition du contenu illégal?
 - « Hard law » ou « soft law »?
 - *Hard law*: mélange de législation nationale/de l'UE
 - *Soft law*
 - Codes de conduite
 - Autorégulation: conditions d'utilisation (qui diffèrent selon les fournisseurs)

2. Détection

Acteurs privés



- Exemple 2 (suite)

- Détection de **contenu illégal en ligne**

- Principes

- **Pas** d'obligation générale de surveillance ou recherche active des faits (art. 8 DSA, règlement sur les services numériques 2022)
 - Mais des obligations accrues (selon le type de fournisseur de services intermédiaires)
 - Ex. évaluation et atténuation des risques, transparence, certaines obligations de coopération avec les autorités judiciaires
 - **Exception**
 - Enquêtes d'initiative volontaires possibles (= détection volontaire)
 - **Attention**: contraintes liées à la vie privée! (ex. directive e-privacy)
 - Jusqu'en avril 2026: exception pour la détection volontaire d'abus sexuel de mineurs

2. Détection

• Exemple 2 (suite)

- Détection de **contenu illégal en ligne**
 - Modération de contenu
 - Par l'IA et des modérateurs humains
 - Dans quelle mesure? Quelle interaction?
 - -> systèmes d'IA à haut risque?
 - Annexe III AI Act? De prime abord, non
 - Incidence négative sur les droits fondamentaux?
 - Transparence?
 - Notifications?
 - Rôle des signaleurs de confiance?
 - Voies de recours?

Acteurs privés

« Main invisible » du secteur privé



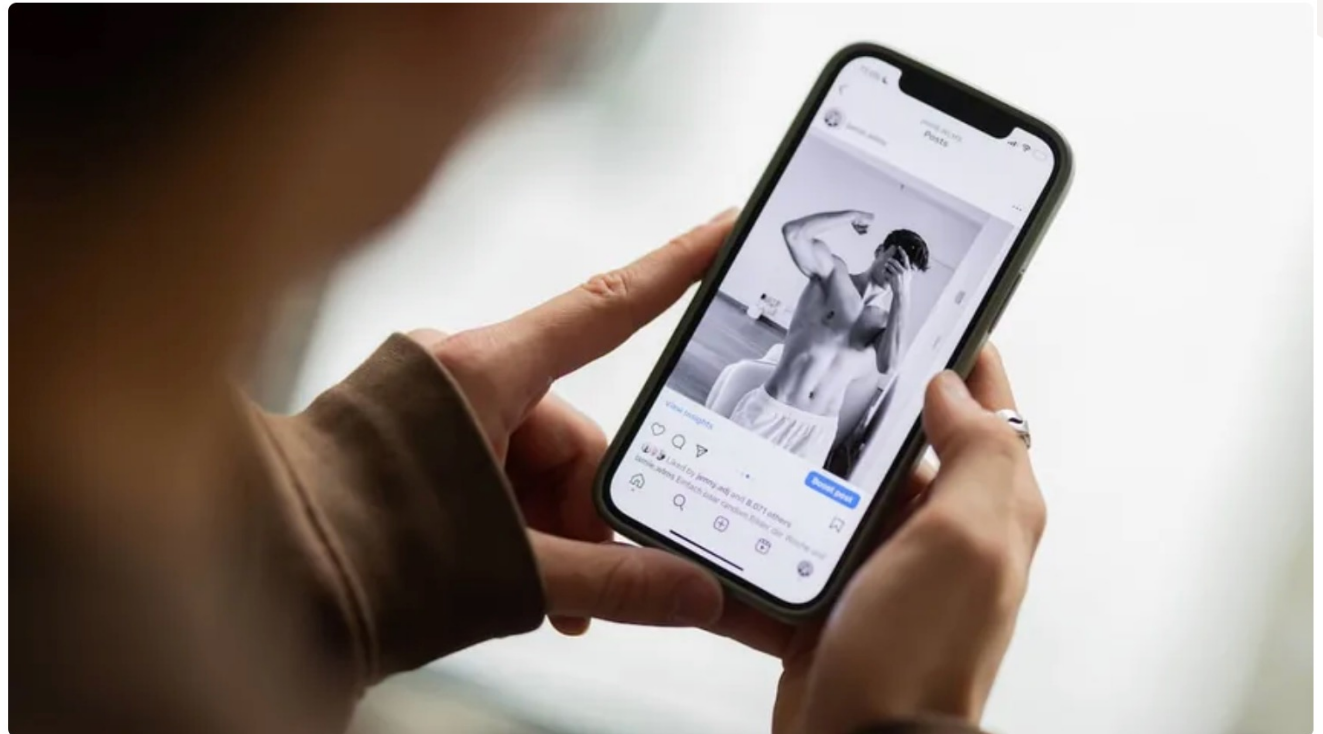
2. Détection

- Exemple 2 (suite)
 - Détection de **contenu illégal en ligne**

<https://dutchtimes.nl/business/dutch-queer-accounts-removed-from-instagram-again-no-explanation-provided/>

Dutch Queer Accounts Removed from Instagram Again: No Explanation Provided

23 April 2026



It is the second time in six months that Dutch accounts have fallen victim to Meta's content moderation. Accounts that have been removed have only been informed that they violated Instagram's guidelines. Some administrators report receiving no explanation at all.

Among those affected are accounts from Amsterdam-based organizations such as The Queer Agenda, Club Church, gavsaua Nieuweziids, and club Tillatec, all of which have been removed from Instagram.

2. Détection

- Exemple 2 (suite)

- Détection de **contenu illégal en ligne**
 - Coopération avec les autorités judiciaires?
 - Indispensable, mais encore mal définie (fragmentation du cadre légal, droit national/UE)
 - Acteurs privés à l'échelle *mondiale* >< autorités judiciaires *nationales*
 - Tensions & risques pour les droits fondamentaux, voire l'état de droit et la démocratie

Acteurs privés



Acteurs privés
comme simples
« gate-keepers »
ou privatisation de
la justice?

2. Détection

Acteurs privés



- Exemple 2 (suite)

- Détection de **contenu illégal en ligne**

M. Walrave, C. Van de Heyning, V. Franssen, C. Mathys, J. Vrielink, M. Giacometti, A. Gilen et O. Gangi, *Cyberviolence: defining borders on permissibility and accountability - @ntidote 2.0. Final Report*, Bruxelles, BELSPO, 2023, 146p.

https://www.belspo.be/belspo/brain2-be/projects/FinalReports/Antidote_FinRep_en.pdf.

3. Prédiction



3. Prédiction

Comment la vidéosurveillance algorithmique a été déployée pendant les Jeux olympiques

A titre d'expérimentation, 485 caméras pilotées par un logiciel d'intelligence artificielle ont fonctionné pendant la quinzaine olympique. La Quadrature du net dénonce un manque de transparence dans le dispositif.

Par Arthur Carpentier

Publié le 14 août 2024 à 09h47 · 🕒 Lecture 3 min. · [Read in English](#)

https://www.lemonde.fr/societe/article/2024/08/14/comment-la-videosurveillance-algorithmique-a-ete-deployee-pendant-les-jeux-olympiques_6280517_3224.html

• « Police prédictive »

- Quoi?
 - Prédiction de faits, de futures infractions
 - Qui, où, quand?
- (>< de décisions judiciaires
 - Autre cours)



The 2002 sci-fi thriller “[Minority Report](#)” depicted a dystopian future where a specialized police unit was tasked with arresting people for crimes they had not yet committed. Directed by Steven Spielberg and based on a short story by Philip K. Dick, the drama revolved around “PreCrime” – a system informed by

Author



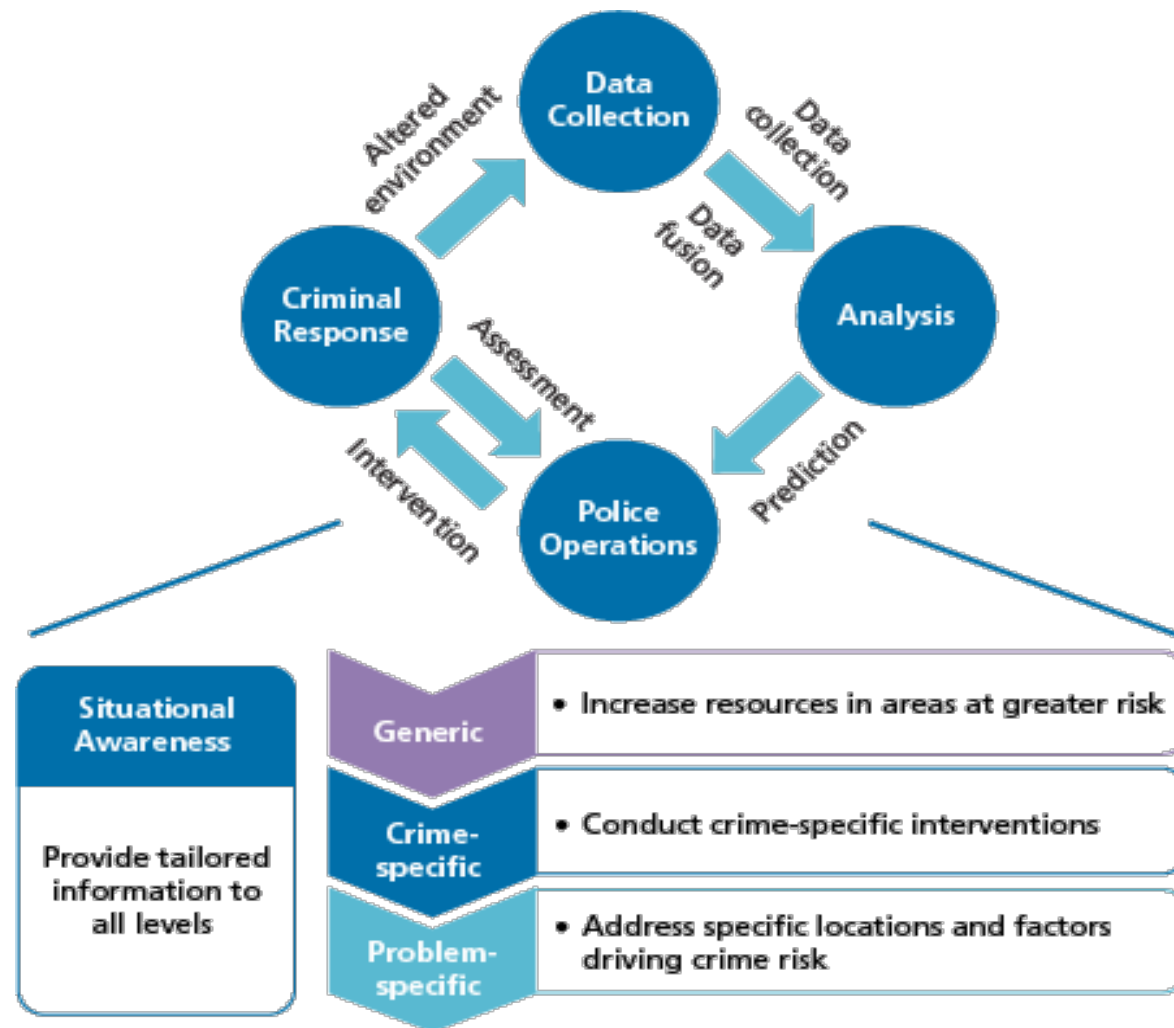
Maria Lungu
Postdoctoral Researcher of Law and Public Administration,
University of Virginia

<https://doi.org/10.64628/AAI.ft5ahuprj>

3. Prédiction

- « Police prédictive »

https://www.rand.org/pubs/research_briefs/RB9735.html



3. Prédiction



- Prédiction de faits, de futures infractions
 - Objectif
 - Évaluation des risques
 - Cibler les interventions
 - Prévenir!
- Rien de nouveau, mais l'IA augmente les possibilités (différence d'échelle)

3. Prédiction

- Exemples de « police prédictive »

- PREDPOL (UK), Criminality Anticipation System or CAS (NL), Palantir (DK), CloudWalk Technology (China)...
- Utilisation répandue!

- Outils liés

- Données biométriques
- Reconnaissance faciale

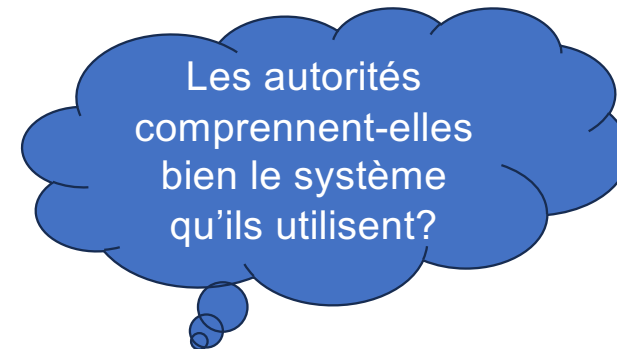


3. Prédiction



• Risques & questions

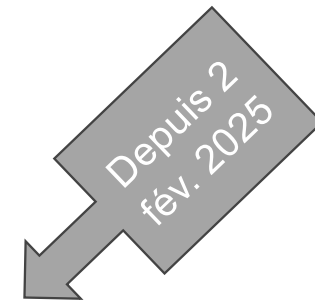
- Effectivité?
 - Discutée
 - Besoin d'évaluation ex post
 - + « cycle de vie » du système d'IA (cf. AI Act)
- Biais
 - Qualité des données, et des algorithmes
- « Self-fulfilling prophecy »
- Surveillance de masse
- Effet déresponsabilisant (« disempowering effects »)
 - D'autres éléments contextuels et préventifs moins pris en compte
- Besoin d'une décision humaine
 - Prohibition d'une décision individuelle purement automatisée (ex. art. 11 Directive « Police »)
 - -> Qu'est-ce qu'une intervention humaine significative/adéquate? (cf. CJUE)



3. Prédiction

• Cadre juridique

- Droits fondamentaux
- RGPD/Directive « Police »
- AI Act:
 - Ex. AI Act interdit le profilage de personnes physiques (art. 5, § 1, d)



« la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation d'un système d'IA pour mener des **évaluations des risques des personnes physiques** visant à évaluer ou à prédire le risque qu'une personne physique commette une infraction pénale, **uniquement sur la base du profilage d'une personne physique ou de l'évaluation de ses traits de personnalité ou caractéristiques**; cette interdiction **ne s'applique pas** aux systèmes d'IA utilisés pour étayer l'évaluation humaine de l'implication d'une personne dans une activité criminelle, qui est déjà fondée sur des faits objectifs et vérifiables, directement liés à une activité criminelle »

Est-ce tjs de la police prédictive??

- Mais **non** applicable s'il s'agit d'une enquête pénale précise, pour étayer une évaluation humaine
 - Dans ce cas, “juste” un système à haut risque
- + précisions et exemples dans les lignes directrices de la Commission européenne (2025, p. 62 et s.): ex. profilage de groupe (ex. terroristes)

4. Enquêtes et poursuites



4. Enquêtes et poursuites

• Exemples

- Justice digitalisée (pas donnée!)
 - Rangements de documents
 - Bases de données
 - Puis: exploitation de ces données pour faciliter la prise de décision?
- Mesures d'enquête/interventions ciblées
 - Collecte de moyens de preuve
 - Saisies
 - Analyse de données
 - Recherche d'informations pertinentes ou de modèles dans de grands ensembles de données
 - "Digital forensics"
 - Ex. Hansken tool aux Pays-Bas, affaire Encrochat
 - Réf.: Publications de M. Galiç (Université d'Amsterdam)
 - Identification de suspects
 - Reconnaissance faciale
 - Données biométriques



Enquête pénale
>< collecte de
« big data »

Distinction
« surveillance de
masse »
>< conservation
de données,
enquêtes ciblées

4. Enquêtes et poursuites



- Risques et questions

- Droit au procès équitable
 - Droits de la défense
 - Accès au système d'IA? Transparence? Accès aux données et aux outputs intermédiaires?
 - Le juge du fond est-il informé?
- Protection des données à caractère personnel
- Droit au respect à la vie privée
- « Blind spots »?
 - La machine voit-elle tout?
 - Problème de langue (et de langage)
- Qui développe les outils d'IA?
 - Coûts?
 - Rôle du secteur privé?
- Responsabilité?
- ...

4. Enquêtes et poursuites

• Cadre juridique

- Directive « Police »: continue à s'appliquer, bien sûr!
- RGPD: idem, acteurs privés

- AI Act

- **Pratiques interdites**

- Ex. certaines formes de reconnaissance faciale (art. 5, § 1, e))

Applicables
depuis 2 fév.
2025

- Mais pas mal **d'exceptions** pour les autorités répressives (ajoutées en phase finale des négociations)

- Déjà exploitées/anticipées par certains législateurs

- Ex. Proposition de loi belge sur l'utilisation de **systèmes d'identification biométrique** à distance en temps réel à des (ou certaines?) fins répressives:
<https://www.lachambre.be/kvvcr/showpage.cfm?section=/flwb&language=fr&cfm=/site/wwwcfm/flwb/flwbn.cfm?lang=F&legislat=56&dossierID=0601>

- **Proposition** d'ajouter une nouvelle interdiction par le Conseil de l'UE (13 mars 2026): outils d'IA capable de générer, de manipuler ou de reproduire du « NCII » (contenu à caractère sexuel non-consenti) ou du « CSAM » (abus sexuel de mineurs)

New

Fais-
able?



4. Enquêtes et poursuites

• Cadre juridique (suite)

- AI Act (suite)

- **Systèmes à haut risque**

- Beaucoup de garanties intéressantes!
 - Transparence
 - Contrôle humain
 - Information /documentation technique
 - Exactitude, sécurité
 - ...

Pas encore applicables, report au 2 déc. 2027

« Wish list » ou future réalité?

- D'autres **systèmes à risque limité** (art. 50 AI Act)

- Destinés à interagir directement avec des personnes physiques
 - Ex. IA générative
 - Obligation de transparence
 - Beaucoup d'**exceptions** pour les autorités répressives
 - Ex. utilisation d'une image « deepfake » lors d'une audition = ok?
 - **Pas** d'obligation d'info!
 - Mais les autres droits s'appliquent évidemment toujours! (ex. égalité des armes, procès équitable)

Applicable à partir du 2 août 2026

4. Enquêtes et poursuites

- Cadre juridique (suite)

- AI Act (suite)

- **Pas** une législation pénale!

- **Faut-il adapter** la procédure pénale et la coopération judiciaire pour tenir compte des défis/risques posés par l'IA?

- High-level Forum on the Future of EU Criminal Justice (rapport final, déc. 2025):

- https://commission.europa.eu/high-level-fora-justice-growth-and-future-eu-criminal-justice_en

- **“While representatives from academia and defence lawyers’ associations called for ambitious, EU level legislative action to address these challenges proactively**, in particular to update and specify certain procedural rights in light of the challenges raised by the use of AI, the **Member States broadly preferred the development of non-legislative measures** (guidelines, training, codes of conduct).”

- “There was **general consensus on the necessity of addressing specific AI risks**, emphasising that AI tools must serve strictly as advisory mechanisms and **must not substitute for human judicial assessment in criminal proceedings**. In particular, the **need to uphold fundamental rights, ensure transparency and traceability, maintain robust human oversight, and ensure equal access to AI tools for both prosecution and defence**, remain critical requirements in the deployment and operational use of such tools.” (rapport final, p. 22)



Réponse
nuancée,
voire
décevante?

5. Conclusions



AI aux fins de détection, de prévention et de poursuite

- De nouvelles opportunités
 - Positives, mais aussi des risques
- Cadre juridique solide = nécessaire
 - A quel niveau?
 - Recherche du juste milieu: pas trop rigide, mais suffisamment de protection?
 - Renforcement/modernisation (du contenu) de certains droits fondamentaux (ex. droits de la défense)
- Formation de tous les acteurs du terrain = aussi indispensable!

Merci de votre attention!

Questions?

vanessa.franssen@uliege.be

