# L'INTELLIGENZA ARTIFICIALE NELL'AMBITO DELL'ATTIVITA' D'IMPRESA

**L'intelligenza artificiale, identità digitale e responsabilità penale**

**17 luglio 2025**

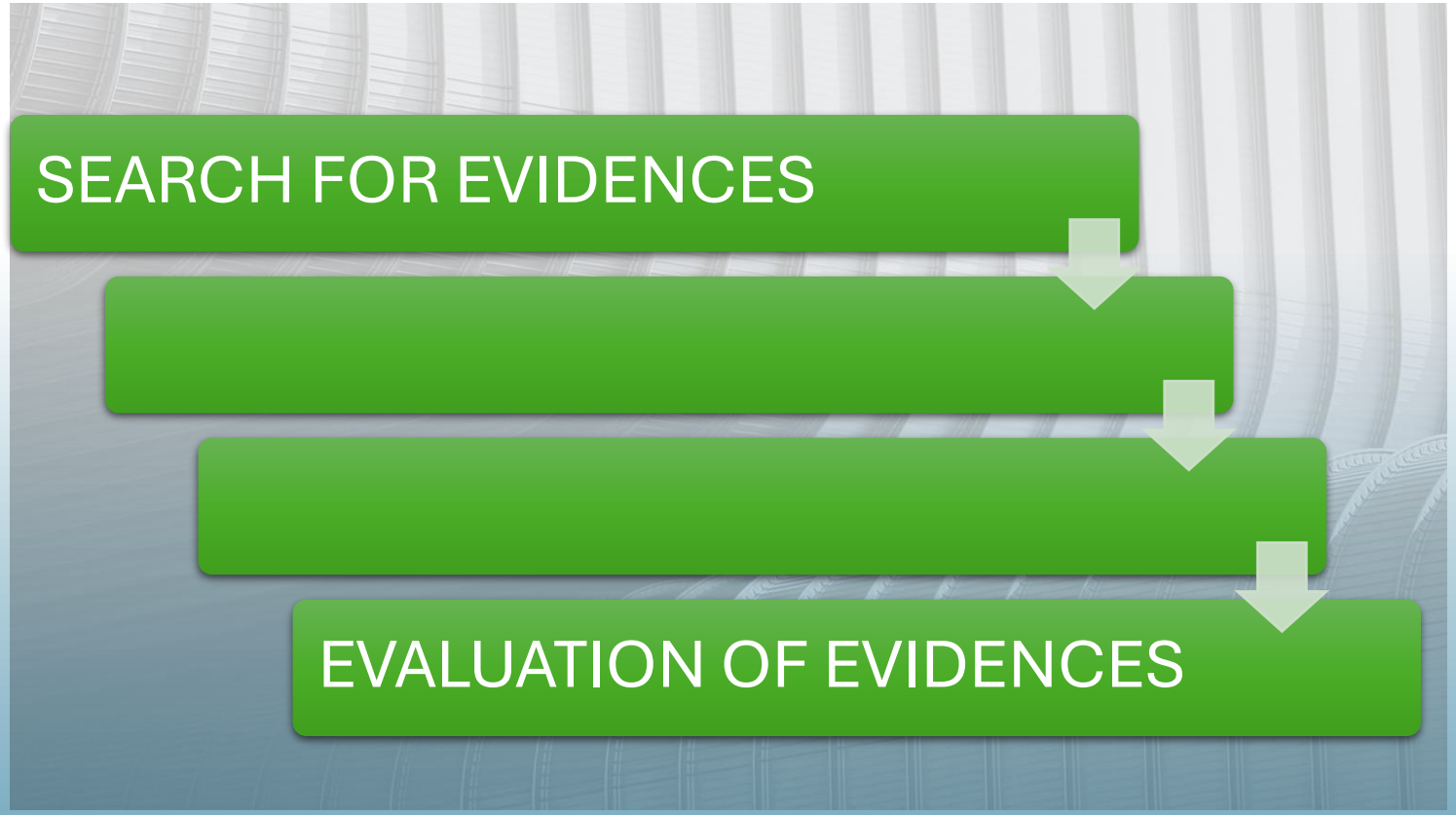
**d.ssa Valentina SELLAROLI**

**Sostituto Procuratore della Repubblica presso il Tribunale di Torino – Criminalità organizzata, cyber crime e antiterrorismo**

# IA E PROCESSO PENALE

L’uso delle nuove tecnologie e degli strumenti di intelligenza artificiale nell’ambito del mondo giudiziario, investigativo e processuale in particolar modo, non scelta aprioristica su principi, ideologie e timori ma necessità da approcciare e gestire in modo produttivo e cautelativo a fronte di diritti fondamentali in gioco

# IA E PROCESSO PENALE



# IA E PROCESSO PENALE


Processing of the characteristics of an audio/human voice signal

Audio enhancement/reconstruction
Voice de-masking
Source separation
Sound transmission

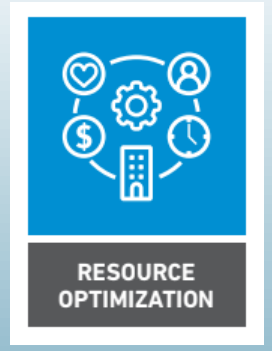
Voice/Audio Profiling

- Speech/Speaker Identification
- Characterization of the psychology of the speaker
- Characterization of the speaker's physiognomy, age, facial structure, etc
- Characterization of the environment (room size, presence of windows, wall material, date of recording based on the fluctuation of the local electricity network, etc.)

# IA E PROCESSO PENALE


Extracting, analyzing, and detecting information from images

Video surveillance systems with machine learning: optimizing operations
Video surveillance systems with deep learning: identification and analysis of targets
Behavioral pattern recognition
Classification of crime scenes
Identification of vehicles/weapons/etc
FDFA: Digital Forensic AI




→

- Map of the areas of greatest interest (hot spots)
- Optimized allocation of police resources
- Optimized routes for territorial control

# IA E PROCESSO PENALE


- Semantic analysis of speech.
- Classification of evidence
- Transcription and understanding of wiretaps

# IA E PROCESSO PENALE


Criminals and terrorists use voice communication on different media. Open source analysis: Leverage voice in public media, typically hate speech or propaganda on Youtube, Facebook, or other social media channels, to track and identify criminal networks.

SERVIZIO POLIZIA SCIENTIFICA
SARI
SISTEMA AUTOMATICO RICONOSCIMENTO IMMAGINI

Enterprise mode that compares a photograph with a large database (in the order of 10 million images) and generates "a list of faces similar to the searched face

https://www.xlaw.it/

XLAW®

Application of the Predictive Police for Urban Security: it allows you to prevent crimes by monitoring where they are scientifically expected to happen and not where they are thought to happen

# IA E PROCESSO PENALE

- The exception of Key Crime, an Italian software used by the Milan Police Headquarters and based not on the analysis of hotspots but on crime linking: prediction not only of where and when but also of who through how (study and reconstruction of the criminal series)

# IA E PROCESSO PENALE

- Easy vs Hard
- Simple vs complex
- Authentic vs Accurate

# IA E PROCESSO PENALE

- Analizzare in maniera strutturata masse di dati enormi in tempi ragionevoli riconoscendo anche il fake e il deep fake
- Decrittare comunicazioni digitali
- Monitorare e ricostruire cluster criminali, serialità di condotte e relazioni, collegamenti tra nodi di reti umane, sociali e criminali ormai sempre più interconnesse nel mondo

# IA E PROCESSO PENALE

Creare, sperimentare, addestrare sistemi complessi pone l'esigenza di individuare risorse e di garantire condizioni di cybersecurity e tutela della privacy ritenute irrinunciabili dalle istituzioni e porre parametri di tutela al di sotto dei quali non è tollerabile il rischio per la tutela delle situazioni fondamentali dell'individuo

# CYBERSECURITY, PRIVACY BY DESIGN E CONCETTO DI RISCHIO

- Nuova regolamentazione europea in tema di obblighi e doveri del «produttore»
- Approccio responsabilizzante: security e privacy by design
- Base dati e addestramento: la genuinità e l'appartenenza dei dati utilizzati come base e per l'addestramento degli strumenti di deep learning; dati vicarianti; dati sintetici; cessione di dati sensibili.

# AI ACT e riforma normativa interna

- Nuove ipotesi delittuose (nuove ipotesi di accessi abusivi ed aumento delle pene per tutte le ipotesi di accesso abusivo aggravato, nuove aggravanti, introduzione della condotta di sottrazione, trasmissione e inaccessibilità dei dati in aggiunta al danneggiamento; inserimento di nuove ipotesi aggravate di estorsione consumate mediante condotte di reati informatici)
- Focus normativo sui data breach, prodromici a moltissimi reati informatici
- Nuovi strumenti di indagine e contrasto alla criminalità informatica: misure cautelari, intercettazioni, i cd. collaboratori informatici, ruolo di coordinamento della DNA
- Necessità di bilanciamento e di previsione di ipotesi tenui nell'ottica di un bilanciamento tra prevenzione speciale, repressione e limitazione dei danni

# AI ACT e riforma normativa interna

- Regolamento UE 2024/1689 art. 3 punto 1: sistema automatizzato progettato per funzionare con livelli di autonomia variabili, che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali

- Il regolamento si riferisce a sistemi di intelligenza artificiale che abbiano capacità inferenziale di generare risultati che possono influenzare ambienti fisici o virtuali attraverso una interazione dinamica e con livelli di autonomia variabile, quindi non i software, per quanto avanzati ed evoluti, ma pur sempre basati sul meccanismo if-this-then-that.

# AI ACT e riforma normativa interna

- art. 15 ddl: riserva di decisione
- Art. 24 delega al Governo per l'adeguamento della normativa nazionale al regolamento UE tra cui apposita disciplina per l'utilizzo di sistemi di intelligenza artificiale per l'attività della polizia: «la regolazione dell'utilizzo di sistemi di IA nelle indagini preliminari nel rispetto delle garanzie inerenti al diritto di difesa e ai dati personali dei terzi, nonché dei principi di proporzionalità, non discriminazione e trasparenza»
- … va da sé che se non si tratta di sistemi di IA (e quindi nel caso di programmi di tipo comparativo deduttivo legati al principio dell'if-then…) questi limiti non si applicano

# AI E PROCESSO PENALE

- Se questi sistemi vengono utilizzati in fase di indagini, gli esiti di questi accertamenti possono entrare a far parte dell'argomentazione che l'organo giudicante dovrà svolgere in sentenza? E in che modo?
- In ogni caso il giudicante dovrà porsi un problema non solo di funzionamento dell'algoritmo (con esclusione quindi delle cd. black box) ma anche della provenienza, completezza, integrità e autenticità dei dati. Come si farà con quegli strumenti che non sono open source? È possibile opporre il segreto della proprietà industriale a fronte della esigenza di conoscenza e replicabilità del processo di valutazione o di conoscenza che lo strumento ha condotto?
- E se è lo strumento stesso a dover essere oggetto di accertamento tecnico? Si pensi ad una consulenza disposta su un software di valutazione di questo tipo…

# AI E PROCESSO PENALE

- Strumenti di IA potranno essere utilizzati per valutare meglio il grado di attendibilità dei testi oculari o per accertare con maggior precisione l'autenticità o la provenienza di un documento
- È opinione prevalente che quando un sistema del genere sia impiegato da autorità giudiziarie in un processo penale non dovrebbe essere mai consentito opporre il segreto industriale sui dati che integrano il codice sorgente
- L'incapacità di stabilire collegamenti causali tra i fatti e l'incapacità di processare i dati in funzione semantica, unite al carattere opaco dei sistemi di autoapprendimento, non consentendo di controllare il procedimento attraverso il quale sono pervenuti a un certo risultato, impediscono di contestare con argomenti razionali il risultato ottenuto: VIOLAZIONE DEL DIRITTO DI DIFESA E DI FORMAZIONE DELLA PROVA IN CONTRADDITTORIO e CARENZA MOTIVAZIONALE

# AI E PROCESSO PENALE

- I canali da approfondire dunque saranno:
  - La cooperazione giudiziaria in senso sempre più dinamico
  - I parametri di valutazione della prova atipica che un sistema di IA potrà produrre: art. 189 c.p.p. il giudice è tenuto ad applicare i criteri legali stabiliti per gli analoghi mezzi di prova tipici ovvero a ricorrere a consolidate massime di esperienza o regole di inferenza secondo una disciplina scientifica (principi della sentenza Franzese: attendibilità della teoria scientifica posta a base della decisione o delle argomentazioni utilizzate per giungere ad essa).

# AI E PROCESSO PENALE: IL PROBLEMA DELL'IDENTITA'

- Ad es. un sistema di analisi comparativa tra dati in termini massivi o di riconoscimento di forme di contraffazione di dati personali (immagine, voce o video) analizzati e confrontati con sistemi di IA: spetterà alla giurisprudenza verificare nell'ambito del principio del contraddittorio l'ammissibilità, l'affidabilità e l'autorevolezza degli elementi probatori derivanti dall'utilizzo di sistemi di IA in fase di indagini tenendo conto anche della provenienza, autenticità, completezza e pertinenza dei dati e delle informazioni che gli ideatori del programma avevano ipotizzato.
- Art. 4 DDL: l'utilizzo di sistemi di IA garantisce il trattamento lecito, corretto e trasparente dei dati personali e la compatibilità con le finalità per le quali sono stati raccolti, in conformità con il diritto dell'Unione europea in materia di dati personali e di tutela della riservatezza

# AI E PROCESSO PENALE: IL PROBLEMA DELL'IDENTITA'

- Rapporto tra il dato e il suo utilizzo: qualunque distorsione di tale rapporto porta alla distorsione del risultato finale
- delega al Governo per definire una disciplina organica relativa all'utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale. Il governo dovrà individuare le ipotesi per le quali è necessario dettare il regime giuridico dell'utilizzo di dati, algoritmi e metodi matematici per l'addestramento di sistemi di IA nonché i diritti e gli obblighi gravanti sulla parte che intenda procedere al suddetto utilizzo, prevedendo altresì strumenti di tutela, di carattere risarcitorio o inibitorio e individuare un apparato sanzionatorio per il caso di violazione

# I CONFINI DELLA RESPONSABILITA' PENALE E IL RISPETTO DEGLI STANDARD DI RISCHIO CONSENTITO

- L'IA come centro di imputazione di responsabilità penale ?
- Criteri per l'individuazione della persona fisica dietro la macchina e distribuzione del carico di responsabilità
- Pluralità di variabili: modalità di programmazione e sviluppo del programma; base informativa utilizzata per svilupparne le funzionalità e il concetto di autonoma elaborazione e di livelli di autonomia variabili
- Metodi di approccio e punti di vista: dalle conseguenze (nel mondo reale o virtuale) alla responsabilità oppure dai principi fondamentali alla ripartizione del rischio
- Derive ultraresponsabiliste e sviluppo: tra l'accettazione del rischio e la tutela dei diritti fondamentali

# I CONFINI DELLA RESPONSABILITA' PENALE E IL RISPETTO DEGLI STANDARD DI RISCHIO CONSENTITO

- Il rischio consentito, la responsabilità penale dolosa e colposa, l'imprevedibilità intrinseca degli effetti
- Il concetto allargato di produttore e il deployer
- Gli usi francamente criminali dell'IA
- L'inquadramento dei sistemi di IA nell'IA Act in base al livello del rischio (inaccettabile, alto, limitato con finalità generali e rischio basso)
- ~~RISCHIO INESISTENTE~~

# I CONFINI DELLA RESPONSABILITA' PENALE E IL RISPETTO DEGLI STANDARD DI RISCHIO CONSENTITO

- Limitazione dei rischi attraverso l'imposizione di un criterio prudenziale
- Rinvio agli organismi di standardizzazione più flessibili e adattabili all'evoluzione tecnologica per l'emanazione di norme cautelari più specifiche e rigide del generico «nei limiti del possibile»

OMBRELLO DI PROTEZIONE ALLA RICADUTA DELLE RESPONSABILITA' PENALI SUI SOGGETTI DELLA FILIERA DI PRODUZIONE E COMMERCIALIZZAZIONE DI SISTEMI DI I.A.

# IL CRITERIO DELLA SORVEGLIANZA UMANA E L'ACCETTAZIONE DEL RISCHIO

- La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali
- No garanzia assoluta: un sistema ad alto rischio è un sistema complesso che funziona con livelli di autonomia variabili per cui è impossibile la previsione in termini di concreta utilità di un intervento umano che possa eliderne in toto gli effetti potenzialmente critici
- In capo a chi va riconosciuta la responsabilità (colposa) per un sistema complesso potenzialmente pericoloso con rischi di effetti dannosi o pericolosi imprevedibili al momento della progettazione? Utilizzatore, produttore, distributore?

# IL CRITERIO DELLA SORVEGLIANZA UMANA E L'ACCETTAZIONE DEL RISCHIO

- DERIVA ULTRARESPONSABILISTA O ESCLUSIONE DELLA SFERA DI RILEVANZA PENALE A FAVORE DI SANZIONI AMMINISTRATIVE E INTERVENTI RISARCITORI?
- Prevedibilità, evitabilità, nesso causale e responsabilità oggettiva
- Responsabilità dell'ente (231/2001) e responsabilità per la base dati

# CONCLUSIONI

- Un certo grado di flessibilizzazione della categoria della responsabilità penale colposa è inevitabile vista l'incompatibilità tra un sistema basato su modelli di tipo probabilistico e un risultato deterministico dell'imputazione dell'evento lesivo
- Adozione di un sistema di gestione della qualità
- Il settore più problematico è quello dei sistemi ad alto rischio per i quali si accetta la possibilità di utilizzo a condizione che vengano garantiti parametri di sicurezza che si scontrano con i limiti della imprevedibilità di sistemi altamente complessi e con forti elementi di autonomia
- La possibile risposta starà prevedere sanzioni penali e profili di responsabilità degli enti riguardo ad una serie di condotte che favoriscono il rischio

# CONCLUSIONI

- Sanzionare omesse o false comunicazioni di informazioni rilevanti per la gestione del rischio
- Incentivare applicazione di sistemi di valutazione e prevenzione dei rischi correlati allo stato dell'arte di ciascun settore
- Prevedere obblighi di verifica e confronto tra produttore / distributore del programma e utilizzatore finale
- Incentivare meccanismi di verifica su dati e informazioni attraverso cui si alimenta il meccanismo di autoapprendimento
- Prevedere obblighi di adeguatezza del programma rispetto alle funzionalità per cui è stato adattato e calibrato in modo da determinare garanzie di affidabilità almeno per gli utilizzatori finali previsti

# CONCLUSIONI

- Tutto ciò senza però rinunciare a chiedere al legislatore europeo e non solo di tenere fermo il criterio della rimproverabilità per l'attribuzione della responsabilità penale perché allargare oltremodo una posizione di garanzia ex art. 40 co. 2 c.p. senza inserirla in un contesto precauzionale e di gestione del rischio è rassicurante ma non si basa su una reale possibilità di vietare comportamenti rimproverabili.
- Necessità di introdurre un sistema di gestione della qualità che valuti la conformità ai requisiti posti dallo stesso regolamento con il coinvolgimento, per la precisazione delle soluzioni tecniche, degli stessi operatori dell'IA
- DELEGA AL GOVERNO: introdurre nuove fattispecie di reato incentrate sull'omessa adozione o adeguamento di misure di sicurezza per produzione, messa in circolazione o utilizzo professionale di sistemi di I.A.; precisare criteri di imputazione della responsabilità penale delle persone fisiche o amministrativa degli enti per gli illeciti inerenti sistemi di I.A. che tenga conto del livello effettivo di controllo di tali sistemi da parte dell'agente

# CONCLUSIONI

- ma chi e come provvederà all'allineamento di questi sistemi complessi, cioè all'affinamento ed avvicinamento degli obiettivi non solo progettuali ma etici in senso ampio?

Non esiste una soluzione tecnica che, imposta, risolva il problema una volta per tutte: la visione promettente per l'allineamento dell'IA con l'essere umano è lo sviluppo di una collaborazione stretta tra umani e intelligenza artificiale in uno scenario in cui l'IA non sostituisce l'umano ma lavora a fianco di esso ampliando le sue capacità senza competere con esse, garantendo un approccio multidisciplinare che integri competenze tecniche, etiche e sociali, salvaguardando inclusivamente le diverse visioni del mondo e delle cose abbandonando il mito della neutralità di questi strumenti e dei loro risultati



www.odcec.torino.it
www.linkedin.com/company/odcec-torino/
www.youtube.com/channel/UCBUHnLEOEHA6YY-MLr8vG8A/videos