CENNI DEL PROCESSO GIURISDIZIONALE E L'ATTIVITÁ DI CONSULENZA

IL PROCESSO GIURISDIZIONALE E L'ATTIVITÁ DI CONSULENZA

ORGANIZZAZIONE DELLO STATO

Basato sul **principio della separazione dei poteri**, di montesquieu, divide i poteri dello stato in tre:

- **Funzione legislativa**
- **Funzione amministrativa**
- **Funzione giurisdizionale**

FUNZIONE LEGISLATIVA
Lo stato pone le norme costitutive dell'ordinamento giuridico

FUNZIONE AMMINISTRATIVA
Lo stato svolge un'attivitá effettiva e concreta diretta al soddisfacimento dei suoi fini immediati.

FUNZIONE GIURISDIZIONALE
Lo stato accerta la volontá normativa da far valere in un caso concreto ed emette le sanzioni, assicurando cosí la certezza del diritto e la reintegrazione dell'ordine giuridico violato

COMPOSIZIONE DELLE CONTROVERSIE

Per accertare l'esistenza o la violazione di un diritto di addice il giudice
Esistono diverse tipologie di giudici:

- **MERITO**
  - **1° Grado**: Giudici di:
    - Tribunale
    - Di pace
    - Corte d'assisi
    - Tribunale amministrativo regionale TAR
  - **2° Grado**:
    - Corte d'appello
    - Corte d'assise d'appello
    - Consiglio di stato
  - **3° Grado**:
    - Suprema corte di cassazione

IL PROCESSO GIURISDIZIONALE

Puó essere di due tipi:

- **Civile e amminstrativo**
- **Penale**

PROCESSO CIVILE E AMMINISTRATIVO
Composto da diverse figure:

- Attore, colui che chiama in giudizio il convenuto:
  - Avvocato difensore
  - Consulente tecnico di parte
- Convenuto, chiamato in causa dall'attore:
  - Avvocato Difensore
  - Consulente tecnico di parte

APPUNTI DIGITAL FORENSICS – SAMUELE CUCUZZA

Il giudice é sempre presente per giudicare i fatti che compongono il processo, insieme al suo team composto da Cancelliere, Ufficiale giudiziario e Consulente Tecnico di ufficio
PROCESSO PENALE
Composto da diverse figure:

- Pubblico ministero, colui che accusa:
  - Polizia giudiziaria
  - Consulente tecnico del PM
- Imputato, colui che viene accusato:
  - Avvocato difensore
  - Consulente tecnico di parte
- Parte civile, colui che viene offeso:
  - Avvocato difensore
  - Consulente Tecnico di parte

CFU E CTP (CONSULENTE TECNICO DI UFFICIO E DI PARTE)

IL CONSULENTE TECNICO
Persona fisica con elevata esperienza e professionalitá che assume l'incarico di effettuare un attivitá tecnica al fine di redigere una perizia

TIPOLOGIE DI CONSULENTE TECNICO
Esistono due tipologie di consulenti tecnici:

- **Consulente Tecnico di Ufficio**: Perito al quale un giudice affida l'incarico. Assume qualifica di pubblico ufficiale
- **Consulente Tecnico di Parte**: Perito che prende l'incarico dalla parte o dal difensore. Produce un rapporto privatistico

La richiesta di iscrizione all'albo professionale deve essere presentata al tribunale presso la cui circoscrizione l'istante risiede. Nel mio caso Catania al link **http://www.tribunalecatania.it/**

NOMINA DEL CTP
La nomina del CTP puó avvenire:

- A **cura del legale** per seguire le attivitá del CTU
- Su diretto incarico ricevuto dalla **parte**

Accordi da prendere:

- Individuare l'ambito dell'incatico
- Stilare un preventivo per il compenso

L'incatrico del CTP non puó essere conferito ad associazioni professionali o di professionisti ma solo ad un singolo individuo
Il CTP puó essere nominato solo se é stato nominato un CTU

CTPM NEL PROCESSO PENALE ART. 359 C.P.P
Il pubblico ministero, quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ognio oprazione tecnica per cui sono necessarie specifiche competenze, puó nominare e avvalersi di consulenti, che non possono rifiutare la loro opera (se iscritti agli albi)
Il consulente puó essere autorizzato dal pubblico ministero ad assistere a singoli atti di indagine.
In sostanza qual'ora al pubblico ministero servisse una figura professionista della Digital Forense e non solo convoca i consulenti iscritti agli albi.

RESPONSABILITÁ DEL CONSULENTE TECNICO
Obbligo di rispettare i principi di **Correttezza** e **Buona fede** e di comportarsi in giudizio con **Lealtá** e **Probitá**

ATTIVITÁ DEL CONSULENTE TECNICO
ART. 194 c.p.c
Il CTP interviene nella attivitá peritali del CTU e puó presentare, per iscritto o a voce, osservazioni e istanze.
ES. Puó chiedere di eseguire una certa analisi che il CTU non aveva previsto

APPUNTI DIGITAL FORENSICS – SAMUELE CUCUZZA

COMPITI DEL CTP

- Evidenziare gli aspetti favorevoli alla propria parte e suggerire le strategie ed espedienti devono adottarsi per contrastare gli eventuali punti sfavorevoli messi in campo dalla controparte
- Assistere la parte nell'eventuale procedimento ricusazione/sostituzione del CTU
- Valutare possibili ipotesi transattive da proporre o ricevute
- Collabora con il difensore per accertare eventuali **cause di nullitá formale o sostanziale** del CTU

Principali cause di nullitá:

- **Innosservanza del principio del contraddittorio**
- **Effettuazione di indagini che eccedono le richieste del quesito o i poteri che la legge conferisce al CTU**

ATTI INVASIVI SU SISTEMI INFORMATICI E TELEMATICI
LEGGE 18 MARZO 2008, N.48
Esegue la convenzione del consiglio d'europa sulla criminalitá informatica, siglata a Budapest il 23 Novembre 2001

Introduce disposizioni correttive ed integrative al codice di procedura penale mediante le quali **nei casi di intervento invasivo sui sistemi informatici e telematici**

Si dovranno adottare **Misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione**

La **copia dei dati** deve avvenire con una **procedura che assicuri la conformitá dei dati copiati e la loro immodificabilitá**

RICERCA DELLA PROVA
Dove cercare una prova:

- **Domicilio Fisico**: Abitazione, ufficio
- **Domicio Informatico**: PC, email, HD, cloud
- **Smarthphone**: Rappresentazione della sfera personale, professionale e della vita di relazione

MODALITÁ DI ACQUISIZIONE DEI DATI
L'acquisizione dei dati avviene tramite la **copia forense** chiamata pure **Bit Stream Image**
Copia Forense: Perfetta riproduzione del contenuto del device

LA PROVA
La parte puó avvalere ció che afferma con **qualunque mezzo di prova concesse dalla legge**
Le prove vengono valutate dal giudice se legali o meno.

APPUNTI DIGITAL FORENSICS – SAMUELE CUCUZZA

CONCETTO DI VERITÁ
Esistono due concetti di veritá:

- **Veritá Processuale**: Risultato del susseguirsi delle **formalitá** descritte nelle **procedure giudiziarie**
- **Veritá Assoluta**: Veritá vera e propria.

CRIMINI INFORMATICI

CRIMINI INFORMATICI

PRINCIPALI BENI MINACCIATI O LESI
I principali beni a rischio minacia o lesione sono:

- **Stato, amministrazioni e servizi pubblici**
- **Patrimonio**
- **Persona** (Integritá Fisica, morale, psicologica, ecc.)
- **Ordine Pubblico**
- **Fede Pubblica**

CYBERCRIME
Chiamati anche crimini informatici, sono quei crimini che vengono commessi tramite un dispositivo informatico
Fattispecie di cybercrime:

- **Hacking**
- **Diffusione di Virus Informatici**
- **CyberStalking**
- **CyberTerrorismo e Propaganda**
- **Diffamazione**
- **Furto d'Identitá, Truffe, Frodi**
- **Pedofilia e reati a sfodo sessuale**

SOFTWARE LEGGE 633/1941 ART. 171 BIS
Punisce con la reclusione e multa:

- Chi **Abusivamente duplica** al fine di trarne **profitto**, programmi per elaboratori protetti SIAE
- Chi predispone o utilizza un qualsiasi mezzo inteso unicamente a consentire o facilitare la **Rimozione albitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma** (Crack o download illegale del software)
- Chi riproduce su supporti non contrassegnati SIAE il contenuto di una banca dati al fine di trarne profitto

ART 635-BIS C.P
Danneggiamento di informazioni. Dati e programmi informatici
Chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui é punito a **querela della persona offesa con la reclusione**

ART 635-QUATER C.P
Danneggiamento di sistemi informatici o telematici

Chiunque mediante le condotte all'articolo 635-bis distrugge, danneggia o rende inutilizzabile **sistemi informatici o telematici** altrui é punito con la reclusione

ART 635-TER C.P
Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilitá
Chiunque danneggia o compromette le funzionalitá di sistemi informazioni, dati e programmi utilizzati dallo **Stato** o da **Enti Pubbliche** o comunque di **Pubblica Utilitá** é punito con la **reclusione da uno a quattro anni.**

DOMICILIO INFORMATICO
ART 615 C.P
Accesso abusivo ad un sistema informatico o telematico
Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza é punito con la reclusione.

ART 615-QUATER C.P
Detenzione o diffusione abusiva di codici di accesso a sistemi informatici e telematici
Chiunque al fine di **procurare a se o ad altri un profitto**, **riproduce**, diffonde, comunica o consegna codici, parole chiave o **altri mezzi idonei all'accesso ad un sistema informatico** o telematico **protetto da misure di sicurezza** é punito con la reclusione e con la multa

VIRUS
ART 615-QUINQUIES C.P
Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.
Chiunque allo **scopo di danneggiare illecitamente un sistema informatico** o telematico, informazioni, dati o programmi in esso contenuti **per favorire l'interruzione totale** o parziale **del suo funzionamento** E **la diffusione dello stesso servizio** é punibile con la reclusione fino a due anni e con la multa sino a 10.329€

FRODE INFORMATICA
ART 640-TER C.P
Chiunque **alterando** in qualsiasi modo **il funzionamento di un sitema informatico**, telematico o **intervenendo senza diritto** con qualsiasi modalitá su **dati, informazioni o profgrammi** contenuti **in un sistema informatico** o telematico **procura a se** o ad altri **profitto con altrui danno** é punibile con reclusione e con la multa

CORRISPONDENZA INFORMATICA
ART 617-QUATER C.P
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche
Chiunque **fraudolentemente intercetta comunicazioni relative a un sistema informatico** o telematico o intercorrenti tra piú sistemi ovvero le **impedisce** o le **interrompe**, é punito con la reclusione.
Stessa pena a chiunque rileva corrispondenza privata altrui.

ART 617-QUINQUIES C.P

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche
Chiunque, **fuori dei casi consentiti dalla legge**, **Installa apparecchiature atte ad intercettare,** impedire o interrompere **comunicazioni** é punito con la reclusione

ART 617-SEXIES C.P
Falsificazone, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche
Chiunque, **al fine di procurare a se o ad altri un vantaggio** o **un danno altrui, forza falsamente** ovvero **altera o sopprime**, tutto o in parte, **il contenuto di una comunicazione relativa ad un sistema informatico** o telematico é punito, **qualora ne faccia uso** o permetta ad altri di farne uso, con la reclusione

PEDOPORNOGRAFIA
ART 600-TER 3° COMMA C.P
Chiunque con qualsiasi mezzo, anche per via telematica, **distribuisce,** divulga, diffonde o pubblicizza il **materiale pornografico**, **finalizzate all'addescamento o allo sfruttamente sessuale di minori degli anni diciotto** é punito con la reclusione e con la multa.
Chi offre o cede ad altri anche a titolo ratuito il materiale pornografico la pena é aumentata
Chiunque assiste a esibizioni o spettacoli pornografici in cui siano conibolti minori di anni diciotto é punito.

REVENGE PORN
ART 612-TER C.P
Diffusione illecita di immagini o video sessualmente espliciti
Chiunque, **dopo averli realizzati o sottratti, invia**, consegna, cede, pubblica o diffonde **immagini o video a contenuto sessualmente esplicito destinati a rimanere privati senza il consenso delle persone rappresentate** é punito con la reclusione e con la multa

RISERVATEZZA DEI DATI

LA TUTELA DELLA RISERVATEZZA E IL TRATTAMENTO DEI DATI PERSONALI NEL GDPR

DISPONIBILITÁ DEL DIRITTO ALLA RISERVATEZZA
La **Riservatezza** é un **Diritto Assoluto** ma **Rinunciabile** attraverso il **Libero Consenso dell'interessato** o di chi ne esercita la patria podestá
Il diritto alla Riservatezza é un diritto disponibili, liberamente negoziabile

TRATTAMENTO DEI DATI PERSONALI NELL'ORDINAMENTO GIURIDICO ITALIANO
LEGGE 675
Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali
Prima legge Italiana sulla protezione dei dati personali

DECRETO LEGISLATIVO 196
Codice in materia di protezione dei dati personali
Rappresenta il primo tentativo al mondo di comporre in maniera organica le innumerevoli disposizioni relative alla tutela dei dati personali

NOZIONE CONTENUTA NEL GDPR
Riservatezza dei dati é oggi intesa come **Diritto di Controllare l'uso e la Circolazione dei propri dati personali** che costituiscono un bene primario della societá dell'informazione

FIGURE CHIAVE
Figure chiave per quanto riguarda in dati personali:

- **Garante**, Supervisore della protezione dei dati
- **Titolare**, Controllore dei dati personali
- **Responsabile Del Trattamento**, Processatore dei dati personali
- **Responsabile della protezione dei dati**, Ufficiale della protezione dei Dati personali
- **Incaricato**, Persone autorizzate al trattamento
- **Interessato**, Persona fisica a cui si riferiscono i dati personali

APPUNTI DIGITAL FORENSICS – SAMUELE CUCUZZA

DATO PERSONALE
Qualsiasi informazione riguardante una persona fisica identificata o identificabile.

Identificabile: Persona fisica che puó essere identificata direttamente, o indirettamente, con un particolare riferimento a un identificativo come:

- **Nome**
- **Numero di identificazione**
- **Ubicazione**
- **Identificativo online**
- **Elementi caratteristici della sua identitá fisica, fisiologica, genetica, psichica, economica, culturale o sociale**

GARANZIE
Esistono due tipi di garanzie della privacy:

- **Privacy by Design**: La protezione dei dati personali viene garantita **fin dalla progettazione**
- **Privacy by Default**: La protezione dei dati personali viene garantita per **impostazione predefinita**

DIRITTO ALL'OBLIO
L'interessato ha il diritto di ottenere dal titolare del trattamento **la Cancellazione dei dati personali che lo riguardano** senza ingiustificato ritardo e il **titolare** del trattamento **ha l'obbligo di cancellare** senza ingiustificato ritardo i **dati personali**

DIRITTO ALLA PORTABILITÁ DEI DATI
L'**interessato ha il diritto di ricevere in un Formato Strutturato, di uso comune e leggibile da dispositivo automatico** i dati personali che lo riguardano forniti ad un **titolare** del trattamento **senza impedimenti da parte del titolare a cui li ha forniti**

DATA BREACH
Il regolamento prevede espressamente **l'obbligo del titolare a notificare la violazione al garante per la protezione dei dati personali, a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertá delle persone fisiche**

AI ACT

ARTIFICIAL INTELLIGENCE ACT

Costituito da **113 articoli, 118 Con. E 13 All.**
La concreta applicazione é scadenzata dopo l'entrata in vigore:

- I divieti relative a pratiche vietate si applicheranno a partire da 6 mesi dopo
- I codici di buone pratiche 9 mesi dopo
- Le norme sui sistemi AI per finalitá generali 12 mesi dopo
- Gli Obblighi per i sistemi ad alto rischio 36 mesi dopo

VISIONE
Tecnologia antropocentrica: **Strumento per le persone con il fine di migliorare il benessere degli esseri umani**
Garantire la sicurezza e i diritti fondamentali delle persone e delle imprese e rafforzare la diffusione, gli investimenti e l'innovazione nell'UE

GOVERNANCE
Ufficio sull'intelligenza artificiale
Responsabile dell'attuazione effettiva dell'AI act:

- **Promuove** l'uso di sistemi affidabili
- **Monitora** l'evoluzione del mercato di settore
- **Coopera** con le autoritá e gli organismi dei singoli stati membri

European Artificial Intelligence Board
Garantirá l'**armonizzazione tra gli stati membri** nell'applicazione dell'AI ACT offrendo consulenza alla commissione e agli stati

APPUNTI DIGITAL FORENSICS – SAMUELE CUCUZZA

Autoritá nazionale per l'Intelligenza Artificiale
Irrogare le sanzioni previste in caso di violazioni. Dovrá esercitare i suoi poteri in modo:

- **Indipendente**
- **Imparziale**
- **Senza Pregiudizi**

Disponendo di risorse:

- **Tecniche**
- **Finanziarie**
- **Umane**
- **Infrastrutture**

Forum Consultivo
Formato da una selezione equilibrata di portatori di interesse ed alcune enti come:

- **Agenzia per i Diritti Fondamentali**
- **Agenzia dell'Unione Europea per la CyberSecurity**
- **Comitato Europeo di Normazione**

Comitato scientifico di esperti indipendenti
Fornirá consulenza e supporto all'AI Office, per quanto riguarda i modelli e i sistemi di AI ad uso generale:

- **Segnalando** possibili **rischi sistematici**
- **Contribuendo** allo **sviluppo** di **strumenti e metodologie per valutare le capacitá dei modelli e dei sistemi AI** ad uso generale

STRUTTURA
L'AI ACT si basa su un sistema di classificazione per determinare il livello di rischio che una tecnologia basata sull'AI potrebbe rappresentare per la **Salute, Sicurezza o diritti fondamentali delle persone**
Sono previsti quattro livelli di rischio:

- **Rischio Inaccettabile**
- **Alto Rischio**
- **Rischio Limitato**
- **Rischio Minimo**

APPLICAZIONI FUORI LEGGE → MINACCE AI DIRITTI DEI CITTADINI

- **Categorizzazione Biometrica**: basata su caratteristiche sensibili
- **Estrapolazione di Immagini Facciali**: Da internet o da registrazioni dei sistemi di telecamere a circuito chiuso per **creare banche dati** di riconoscimento facciale
- **Riconoscimento delle emozioni**: Sul luogo di lavoro o nelle scuole
- **Credito Sociale**
- **Polizia Predittiva**: Basata sulla profilazione o sulla valutazione delle caratteristiche di una personale
- **Manipolazione del Comportamento**: Umano o sfruttamento delle vulnerabilitá delle persone

FORZE DELL'ORDINE
Non potranno dare ricorso a sistemi di identificazione biometrica salvo i casi espressamente previsti dalla legge

APPUNTI DIGITAL FORENSICS – SAMUELE CUCUZZA

L’identificazione in tempo reale potrá essere utilizzata solo se saranno rispettate le garanzie rigorose. ES. Uso limitato nel tempo e nello spazio e previa autorizzazione giudiziaria o amministrativa
ES. La ricerca di una persona scomparsa o la prevenzione di un attacco terroristico

SISTEMI AD ALTO RISCHIO
Destinati ad essere utilizzati come **componenti di sicurezza di prodotti.**
Rientrano in **Settori Critici** se presentano un rischio significativo di danno per la salute umana, la sicurezza o i diritti fondamentali delle persone fisiche

REQUISITI E OBBLIGHI PER ACCEDERE AL MERCATO DELL’UE

- **Adozione di sistemi di gestione dei rischi**
- **Elevata qualitá dei set di dati che alimentano il sistema**
- **Adozione di documentazione tecnica recante tutte le informazioni necessaria alle autoritá per valutare la conformitá dei sistemi si AI ai requisiti**
- **Conservazione delle registrazioni degli eventi**
- **Trasparenza e fornitura di informazioni e misure di sorveglianza umana**
- **Adeguati livelli di accuratezza, robustezza, cybersicurezza**

SISTEMI A RISCHIO LIMITATO
Per i sistemi che interagiscono con gli individui, riconoscimento delle emozioni e di categorizzazione biometrica, che generano o manipolano contenuti vi é **l’obbligo di informare l’utente che sta interagendo con un sistema di intelligenza artificiale o del fatto che un particolare contenuto é stato creato attraverso l’intelligenza artificiale**

REGIME SANZIONATORIO
L’AI ACT prevede sanzioni molto gravi in caso di mancato rispetto delle disposizioni vigenti
Da 10 a 40 milioni di euro o dal 2% al 7% del fatturato annuo globale dell’azienda.
La presentazione di documentazione falsa o fuorviante alle autoritá di regolamentazione é sanzionata severamente

SCHEMA DI DISEGNO DI LEGGE RECANTE DISPOSIZIONI E DELEGA AL GOVERNO IN MATERIA DI INTELLIGENZA ARTIFICIALE

CAPO 1 – PRINCIPI E FINALITÀ

ART 1 FINALITÁ E AMBITO DI APPLICAZIONE

Questa legge regola l'uso dell'intelligenza artificiale (IA) promuovendone un utilizzo corretto, **trasparente e responsabile**, con un'attenzione particolare ai diritti umani e ai rischi economici e sociali. Le sue disposizioni devono essere conformi alle leggi dell'Unione Europea.

ART 2 DEFINIZIONI

Un sistema di intelligenza artificiale è un sistema automatizzato con diversi livelli di autonomia che può adattarsi e generare output (come previsioni, contenuti o decisioni) influenzando ambienti fisici o virtuali. Per dato si intende qualsiasi rappresentazione digitale di informazioni, inclusi suoni, immagini e video.
I modelli di intelligenza artificiale sono modelli che riconoscono schemi nei dati, eseguono vari compiti e possono essere integrati in diversi sistemi o applicazioni.

ART 3 PRINCIPI GENERALI

La ricerca e l'applicazione dell'IA devono rispettare i diritti fondamentali, le leggi dell'Unione Europea e i principi di trasparenza, sicurezza e non discriminazione.

Lo **sviluppo dell'IA deve garantire la correttezza e la qualità dei dati e dei processi utilizzati**. L'IA deve **rispettare l'autonomia umana e prevenire danni, mantenendo la conoscibilità e spiegabilità**.
L'uso dell'IA non deve compromettere la democrazia. La cybersicurezza è essenziale per tutto il ciclo di vita dell'IA, con controlli di sicurezza specifici. La legge assicura alle persone con disabilità pieno accesso all'IA senza discriminazioni, in linea con la Convenzione ONU sui diritti delle persone con disabilità.

ART 4 PRINCIPI IN MATERIA DI INFORMAZIONE E DI RISERVATEZZA DEI DATI PERSONALI
L'IA deve essere utilizzata senza compromettere la libertà di espressione e il pluralismo dei media, garantendo obiettività e imparzialità.
Il **trattamento dei dati personali deve essere lecito**, corretto e trasparente, rispettando le leggi europee. Le informazioni sul trattamento dei dati devono essere chiare e semplici per permettere agli utenti di comprendere e opporsi a usi impropri.
L'accesso all'IA per minori di 14 anni richiede il consenso dei genitori,
mentre **i minori tra 14 e 18 anni possono dare il proprio consenso** se le informazioni sono facilmente comprensibili.

ART 5 PRINCIPI IN MATERIA DI SVILUPPO ECONOMICO
L'Articolo 5 **stabilisce i principi per lo sviluppo economico legato all'intelligenza artificiale**. **Lo Stato e le autorità pubbliche devono promuovere l'uso dell'IA per migliorare la produttività nei settori produttivi e favorire nuove attività economiche**, aumentando la competitività nazionale e la sovranità tecnologica. **Devono anche creare un mercato dell'IA innovativo e competitivo, facilitare l'accesso a dati di alta qualità per le imprese e la comunità scientifica**, e orientare le piattaforme di e procurement delle amministrazioni pubbliche a privilegiare soluzioni che garantiscono la localizzazione dei dati in Italia e alti standard di trasparenza nello sviluppo di applicazioni basate sull'IA.

ART 6 PRINCIPI IN MATERIA DI SICUREZZA E DIFESA NAZIONALE
L'Articolo 6 **stabilisce che le attività, come quelle svolte dagli organismi di sicurezza e dalle forze armate, sono escluse dall'ambito di applicazione della legge sull'intelligenza artificiale, pur rispettando i diritti fondamentali e la Costituzione**.
Lo sviluppo di sistemi di IA deve rispettare le condizioni previste, e i trattamenti di dati personali per scopi di sicurezza nazionale seguono le leggi specifiche vigenti.
Le modalità di applicazione dei principi della legge alle attività di sicurezza nazionale saranno definite tramite regolamenti specifici.

CAPO 2 – DISPOSIZIONI DI SETTORE

ART 7 USO DELL'INTELLIGENZA ARTIFICIALE IN AMBITO SANITARIO E DI DISABILITÁ

L'IA deve migliorare il sistema sanitario e prevenire malattie rispettando i diritti personali e la protezione dei dati.

Non può discriminare nell'accesso alle cure sanitarie.

I pazienti devono essere informati sull'uso dell'IA e sui suoi vantaggi diagnostici e terapeutici.

La legge promuove l'IA per migliorare la vita delle persone con disabilità, facilitandone l'accessibilità e l'inclusione sociale. L'IA supporta la prevenzione, diagnosi e cura, ma le decisioni finali spettano ai medici. I sistemi di IA e i dati sanitari devono essere affidabili e aggiornati per ridurre errori.

ART 8 RICERCA E SPERIMENTAZIONE SCIENTIFICA NELLA REALIZZAZIONE DI SISTEMI DI INTELLIGENZA ARTIFICIALE IN AMBITO SANITARIO

L'Articolo 8 **permette l'uso dei dati personali per la ricerca scientifica nell'ambito sanitario, senza scopo di lucro**.
Questi trattamenti devono essere approvati dai comitati etici e comunicati all'Autorità Garante per la Protezione dei Dati, ma possono avvenire senza ulteriori consensi se i dati sono anonimizzati. L'Autorità Garante mantiene i suoi poteri di supervisione e sanzioni su tali trattamenti.

ART 9 DISPOSIZIONI IN MATERIA DI FASCICOLO SANITARIO ELETTRONICO, SISTEMI DI SORVEGLIANZA NEL SETTORE SANITARIO E GOVERNO DELLA SANITÁ DIGITALE
L'Articolo 9 **istituisce una piattaforma di intelligenza artificiale nel settore sanitario gestita dall'AGENAS per supportare la cura dei pazienti**.
Utilizza dati trasferiti dai titolari del trattamento, ed è soggetta a valutazioni e pareri preventivi per garantire la sicurezza e la protezione dei dati dei pazienti, senza aggiungere nuovi oneri finanziari pubblici.

ART 10 DISPOSIZIONI SULL'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE IN MATERIA DI LAVORO
L'articolo 10 **stabilisce che l'uso dell'intelligenza artificiale sul lavoro mira a migliorare le condizioni dei lavoratori e la produttività**, nel rispetto delle leggi dell'Unione Europea.
Deve essere sicuro, trasparente e non compromettere la dignità umana né violare la privacy dei dati personali.
Il datore di lavoro deve informare i dipendenti sull'utilizzo dell'IA secondo le disposizioni di legge.
L'IA nell'ambito lavorativo deve rispettare i diritti dei lavoratori senza discriminazioni di nessun tipo, conformemente alle leggi dell'Unione Europea.

ART 11 OSSERVATORIO SULL'ADOZIONE DI SISTEMI DI INTELLIGENZA ARTIFICIALE NEL MONDO DEL LAVORO
L'Articolo 11 **istituisce un Osservatorio presso il Ministero del Lavoro e delle Politiche Sociali per monitorare l'adozione dei sistemi di intelligenza artificiale nel lavoro**.
Ha il **compito di definire una strategia, monitorare l'impatto sul mercato del lavoro e promuovere la formazione dei lavoratori e dei datori di lavoro sull'IA**.
La sua creazione e operatività non generano nuovi costi per la finanza pubblica.

ART 12 DISPOSIZIONI IN MATERIA DI PROFESSIONI INTELLETUALI
L'Articolo 12 **stabilisce che l'utilizzo dei sistemi di intelligenza artificiale nelle professioni intellettuali è consentito solo per attività di supporto e strumentali, con il lavoro intellettuale prevalente**.
Per garantire la fiducia tra professionista e cliente, le informazioni sui sistemi AI utilizzati devono essere comunicate in modo chiaro e completo al cliente.

ART 13 PRINCIPI IN MATERIA DI PUBBLICA AMMINISTRAZIONE
L'Articolo 13 **stabilisce che le pubbliche amministrazioni utilizzano l'intelligenza artificiale per migliorare l'efficienza, ridurre i tempi dei procedimenti e aumentare la qualità dei servizi ai cittadini e alle imprese**.
Devono garantire trasparenza sul funzionamento e tracciabilità dell'uso dell'IA.

L'IA è utilizzata in modo strumentale e di supporto, rispettando l'autonomia e il potere decisionale della persona responsabile dei provvedimenti.
Le amministrazioni adottano misure per garantire un uso responsabile dell'IA e sviluppare le competenze degli utilizzatori.

ART 14 UTILIZZO DELL'INTELLIGENZA ARTIFICIALE NELL'ATTIVITÁ GIUDIZIARIA
L'Articolo 14 **regola l'uso dell'intelligenza artificiale nell'ambito giudiziario. Limita l'impiego dei sistemi AI all'organizzazione del lavoro giudiziario e alla ricerca legale**.
Il Ministero della giustizia disciplina l'uso nei tribunali ordinari, mentre per altre giurisdizioni si segue la normativa specifica. La decisione sull'interpretazione della legge e altri aspetti cruciali rimane sempre nelle mani del magistrato.

ART 15 MODICHE AL CODICE DI PROCEDURA CIVILE
L'Articolo 15 **propone una modifica al Codice di procedura civile, aggiungendo un riferimento specifico alle cause relative al funzionamento di un sistema di intelligenza artificiale dopo la frase "esecuzione forzata"**.

ART 16 UTILIZZO DELL'INTELLIGENZA ARTIFICIALE PER IL RAFFORZAMENTO DELLA CYBERSICUREZZA NAZIONALE
L'Articolo 16 **modifica il decreto-legge del 14 giugno 2021, introducendo la promozione e lo sviluppo di iniziative, comprese quelle di partenariato pubblico-privato, per valorizzare l'intelligenza artificiale nel rafforzamento della cybersicurezza nazionale**.

CAPO 3 – STRATEGIA NAZIONALE, AUTORITÀ NAZIONALE E AZIONI DI PROMOZIONE

ART 17 STRATEGIA NAZIONALE PER L'INTELLIGENZA ARTIFICIALE
L'Articolo 17 **istituisce una strategia nazionale sull'intelligenza artificiale, coordinata dalla Presidenza del Consiglio dei ministri, per promuovere la collaborazione tra settore pubblico e privato nello sviluppo e nell'adozione dell'IA**, oltre a favorire la ricerca e l'innovazione nel settore. La strategia è approvata dal Comitato interministeriale per la transizione digitale e monitorata annualmente con rapporti alle Camere.

ART 18 AUTORITÁ NAZIONALI PER L'INTELLIGENZA ARTIFICIALE
L'Articolo 18 **istituisce l'Agenzia per l'Italia Digitale (AgID) e l'Agenzia per la Cybersicurezza Nazionale (ACN) come Autorità nazionali per l'intelligenza artificiale**.

AgID promuove l'innovazione e sviluppo dell'IA, mentre **ACN è responsabile della vigilanza sui sistemi di IA per garantire la cybersicurezza**.
Entrambe **gestiscono spazi di sperimentazione conformi alle normative. Assicurano il coordinamento tra di loro e con altre autorità,** con un Comitato di coordinamento presso la Presidenza del Consiglio dei ministri. **Le competenze del Garante per la protezione dei dati personali rimangono invariate**.

ART 19 APPLICAZIONE SPERIMENTALE DELL'INTELLIGENZA ARTIFICIALE AI SERVIZI FORNITI DAL MANISTERO DEGLI AFFARI ESTERI E DELLA COOPERAZIONE INTERNAZIONALE
L'Articolo 19 **autorizza una spesa annua di €300.000 per ciascuno degli anni 2025 e 2026 per progetti sperimentali che applicano l'intelligenza artificiale ai servizi del Ministero degli Affari Esteri e della Cooperazione Internazionale.**

ART 20 MISURE DI SOSTEGNO AI GIOVANI E ALLO SPORT
L'Articolo 20 **apporta modifiche e aggiunte per promuovere l'impiego dell'intelligenza artificiale in vari contesti. Aggiunge requisiti relativi alla ricerca in intelligenza artificiale per alcune categorie di studenti, facilita l'accesso alle attività di apprendimento per studenti dotati, e promuove l'accessibilità e l'innovazione nell'ambito dello sport** attraverso l'utilizzo dei sistemi di intelligenza artificiale.

ART 21 INVESTIMENTI NEI SETTORI DI INTELLIGENZA ARTIFICIALE, DELLA CYBERSICUREZZA E CALCOLO QUANTISTICO
L'Articolo 21 **permette investimenti fino a un miliardo di euro per supportare imprese nell'ambito dell'intelligenza artificiale, della cybersicurezza e del calcolo quantistico, tramite il Fondo di sostegno al venture capital**.
La struttura della Presidenza del Consiglio dei ministri e l'Agenzia per la cybersicurezza nazionale partecipano senza compenso agli organi di governo dei fondi di venture capital.

ART 22 DELEGHE AL GOVERNO IN MATERIA DI INTELLIGENZA ARTIFICIALE
L'Articolo 22 **delega al Governo l'adozione di decreti legislativi entro dodici mesi per adeguare la normativa nazionale al Regolamento europeo sull'intelligenza artificiale**.
Specifica principi e criteri direttivi, incluso l'istituzione di autorità competenti, percorsi di alfabetizzazione, formazione professionale, e disciplina per l'uso illecito dell'intelligenza artificiale. Questi decreti devono rispettare principi di inibizione della diffusione illecita, introduzione di reati, e revisione della normativa vigente.

CAPO 4 – DISPOSIZIONI A TUTELA DEGLI UTENTI E IN MATERIA DI DIRITTO D'AUTORE

ART 23 IDENTIFICAZIONE DEI CONTENUTI TESTUALI, FOTOGRAFICI, AUDIOVISIVI E RADIOFONICI PRODOTTI DA SISTEMI DI INTELLIGENZA ARTIFICIALE
Il decreto legislativo 8 novembre 2021 n. 208 viene modificato per includere disposizioni riguardanti l'identificazione dei contenuti prodotti da sistemi di intelligenza artificiale.

Questi **contenuti** devono essere **chiaramente contrassegnati con un segno identificativo (watermark) quando vengono diffusi da fornitori di servizi audiovisivi e radiofonici su qualsiasi piattaforma, incluso il video on demand e lo streaming**.
L'identificazione deve essere visibile all'inizio e alla fine del contenuto, nonché ad ogni ripresa dopo interruzioni pubblicitarie. **L'identificazione non è richiesta per contenuti chiaramente creativi, satirici, artistici o fittizi**.
L'Autorità è incaricata di promuovere forme di regolamentazione volontaria in collaborazione con i fornitori di servizi e piattaforme.

ART 24 TUTELA DEL DIRITTO D'AUTORE DELLE OPERE GENERATE CON L'AUSILIO DELL'INTELLIGENZA ARTIFICIALE
Il diritto d'autore delle opere generate con l'ausilio dell'intelligenza artificiale è tutelato mediante modifiche alla legge 22 aprile 1941, n. 633.
Queste modifiche chiariscono che le opere create con l'intervento umano creativo, rilevante e dimostrabile, anche con l'ausilio di strumenti di intelligenza artificiale, sono considerate opere dell'ingegno.
Inoltre, viene consentita la riproduzione e l'estrazione di opere o altri materiali attraverso modelli e sistemi di intelligenza artificiale, in conformità con gli articoli esistenti sulla riproduzione.

CAPO 5 – DISPOSIZIONI FINALI

ART.25 MODIFICHE AL CODICE PENALE ED ALTRE DISPOSIZIONI PENALI

Le modifiche al Codice penale includono l'introduzione di disposizioni riguardanti l'uso di sistemi di intelligenza artificiale nei reati. Queste modifiche comprendono l'**aggiunta di nuovi articoli e l'aggiustamento di disposizioni esistenti per affrontare i crimini che coinvolgono l'impiego di intelligenza artificiale**.
Ad esempio, vengono specificati i casi in cui l'utilizzo di sistemi di intelligenza artificiale può aggravare le conseguenze del reato o ostacolare la difesa pubblica o privata.
Le pene per reati come diffamazione, truffa, furto di dati online e altri sono aumentate se commessi mediante l'impiego di sistemi di intelligenza artificiale.

Chiunque cagiona ad altri un danno ingiusto, mediante invio, consegna, cessione, pubblicazione o comunque diffusione di immagini o video di persone o di cose ovvero di voci o suoni in tutto o in parte falsi, generati o alterati mediante l'impiego di sistemi di intelligenza artificiale, atti a indurre in inganno sulla loro genuinità, è punito con la reclusione da uno a cinque anni.

ART 26 DISPOSIZIONI FINANZIARIE
L'articolo 26 **stabilisce che l'attuazione della legge non deve causare nuovi o maggiori oneri finanziari per la finanza pubblica**.
Le amministrazioni pubbliche coinvolte devono garantire l'adempimento delle disposizioni utilizzando le risorse umane, strumentali e finanziarie disponibili secondo la legislazione attuale.

FINE CORSO DF 2023/2024
SAMUELE CUCUZZA