

**CORSO DI FORMAZIONE E AGGIORNAMENTO PER OPERATORI DI
POLIZIA GIUDIZIARIA
NUOVE TECNOLOGIE, DATI BIOMETRICI E PROCEDIMENTO PENALE**

QUIZ DI AUTOVALUTAZIONE

Modulo “La disciplina europea dell’*AI Act*”

1) L’ambito applicativo territoriale dell’*AI Act* si fonda principalmente:

- A) Sulla nazionalità dell’operatore
- B) Sul luogo di produzione del sistema
- C) Sulla localizzazione del *server*
- D) Sugli effetti prodotti nel territorio dell’Unione

2) Nella disciplina dell’*AI Act*, i sistemi ad alto rischio sono caratterizzati da:

- A) Assenza di obblighi specifici
- B) Obblighi di sola trasparenza
- C) Obblighi stringenti e valutazione di conformità *ex ante*
- D) Divieto assoluto

3) In base all’*AI Act*, l’identificazione biometrica remota in tempo reale negli spazi pubblici per finalità di *law enforcement* è:

- A) Considerata a rischio minimo
- B) In linea di principio vietata, con eccezioni tassative
- C) Sempre consentita
- D) Sempre vietata senza eccezioni

Modulo “Prove penali e *FRS*”

1) Barrare l’opzione corretta:

- A) L’impiego di sistemi di riconoscimento facciale nell’ambito delle indagini penali è sempre ammesso a discrezione degli operanti
- B) In quanto ingerenza nel diritto al rispetto della vita privata, l’impiego dei sistemi di riconoscimento facciale a fini di indagine penale deve essere regolamentato dalla legge
- C) Non si può fare alcun uso delle informazioni raccolte attraverso l’impiego di sistemi di riconoscimento facciale
- D) I sistemi di riconoscimento facciale sono disciplinati nel codice di procedura penale

2) Il regolamento 2024/1689/UE (c.d. *AI Act*):

- A) Vieta in ogni caso il ricorso a sistemi di riconoscimento facciale *real time*
- B) Ammette sempre l'utilizzo di sistemi di riconoscimento facciale in differita senza alcun tipo di condizione
- C) Ammette l'uso di sistemi di riconoscimento facciale solo durante le indagini penali
- D) Consente il ricorso a sistemi di riconoscimento facciale *real time* anche a scopi di prevenzione nel rispetto del principio di proporzionalità

3) L'uso come prova in giudizio dei risultati generati dal *software* di riconoscimento facciale:

- A) È sempre ammesso senza il rispetto di condizioni di sorta
- B) È sempre vietato in quanto il riconoscimento facciale non è un mezzo di prova previsto dalla legge
- C) Soggiace alle formalità previste dall'art. 213 c.p.p. per la ricognizione di persone
- D) Al di là dell'inquadramento preferibile del riconoscimento facciale nelle categorie probatorie esistenti, è subordinato al rispetto del principio costituzionale della formazione della prova nel contraddittorio tra le parti

4) Il principio di parità delle parti:

- A) Esige che siano noti ed accessibili i principi di funzionamento tecnico dello strumento di riconoscimento facciale perché lo stesso generi conoscenze ammissibili come prova
- B) Preclude sempre il ricorso al riconoscimento facciale
- C) Non si applica alle prove atipiche
- D) Riguarda solo la prova documentale

5) Per "identificazione" si intende:

- A) Un raffronto di tipo 1:n
- B) il riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati
- C) Né A), né B)
- D) Sia A), sia B)

6) Come ridurre il rischio di *confirmation bias*

- A) Adottare *policy* di tipo *blind*
- B) Fare conoscere con precisione *score* e *ranking* di ogni individuo nella *candidate list*
- C) Rendere noti eventuali ulteriori elementi a supporto del risultato (ad es., se l'individuo è stato identificato con altri mezzi)
- D) Porre una unica affermazione da accertare (es. l'immagine estratta dalle registrazioni dell'impianto di sorveglianza raffigura l'indagato/imputato?)

Modulo “wearable devices”

1) Quale tra le seguenti frasi è corretta?

- A) Tutte le metriche estratte dagli smartwatch sono affidabili e accurate al 100%
- B) La frequenza cardiaca è la metrica che ha dimostrato un'accuratezza peggiore
- C) La frequenza cardiaca è la metrica che ha dimostrato un'accuratezza più alta (in ogni caso tutte le metriche vanno considerate nel loro contesto e con il loro grado di affidabilità)
- D) Il dispendio energetico è utile per un'indagine forense visto che è una misura del tempo trascorso nel letto senza dormire

2) Nel corso di un procedimento penale, quale delle seguenti condotte dell'indagato-utente di dispositivo elettronico non rientra nell'ambito di applicazione del principio *nemo tenetur se detegere*?

- A) Consegnare i dati contenuti nel dispositivo
- B) Sbloccare il dispositivo senza rivelare la *password* all'autorità procedente
- C) Comunicare agli inquirenti la propria *password* alfanumerica
- D) Sbloccare il dispositivo tramite riconoscimento facciale

3) I dati estratti dagli indossabili sono utili all'indagine perché:

- A) Consegnano agli investigatori una fotografia impassibile della realtà
- B) Producono dati, da esaminare tuttavia con estrema cautela e da contestualizzare attentamente
- C) Non sono mai manipolabili, nemmeno se dotati di software risalenti e mai aggiornati
- D) Gli originali sono sempre disponibili ed è estremamente facile tracciare ogni passaggio delle elaborazioni successive, così come richiesto dagli standard dell'informatica forense

Modulo “banche dati e circolazione transnazionale”

1) Qual era la funzione originaria della banca dati Eurodac?

- A) Agevolare l'identificazione degli autori di reati
- B) Contrastare la criminalità transnazionale
- C) Agevolare lo svolgimento delle procedure di asilo

2) A chi deve rivolgersi l'autorità designata di uno Stato membro per procedere a un confronto con i dati contenuti nel *database* Eurodac?

- A) Al punto di accesso nazionale
- B) All'autorità di verifica dello Stato membro
- C) Può procedere autonomamente al confronto dei dati

3) Il regolamento Prüm presenta:

- A) Un'architettura ibrida
- B) Una struttura totalmente centralizzata
- C) Una soluzione completamente decentrata

4) Ai fini della prevenzione, dell'indagine e dell'accertamento di quali reati può essere avviata la procedura di consultazione e scambio delle immagini facciali?

- A) Di tutti i reati
- B) Dei reati punibili con una pena detentiva massima di almeno sei mesi ai sensi della legge dello Stato membro richiedente
- C) Dei reati punibili con una pena detentiva massima di almeno un anno ai sensi della legge dello Stato membro richiedente