Nuove tecnologie e Studio digitale

La dimensione cibernetica del diritto penale: dai reati informatici al delitto di deepfake

di **Emanuele Nagni**

La rivoluzione cibernetica della società, iniziata con l'avvento dell'informatica e oggi proseguita con l'automazione e l'intelligenza artificiale, negli anni ha sospinto l'ordinamento verso un profondo rinnovamento giuridico. Così, a seguito degli impulsi di respiro sovranazionale e per far fronte a situazioni di incertezza e pericolosi vuoti normativi, il legislatore penale è nel tempo intervenuto con nuove fattispecie di reato di pari passo con l'avanzamento del progresso tecnico-scientifico.

Con la nozione di *diritto penale dell'informatica*, allo stato, non ci si riferisce solamente alla normativa codicistica e alla legislazione speciale dettate in materia, perché la linea da perseguire appare tanto in evoluzione da lasciar insorgere l'esigenza di riconsiderare il ramo penale dell'ordinamento in base alla nuova spinta tecnologica operata dalla **diffusione capillare di strumenti tecnologici** sempre più evoluti ed efficienti.

Invero, il funzionamento di tali sistemi incide direttamente sulle relazioni interpersonali e sulla dimensione pubblica e privata dell'economia, della cultura e della realtà socio-politica e, in ambito nazionale e sovranazionale, il primo elemento da considerare nell'approccio giuridico alla **rivoluzione cibernetica** è quello dell'***automation*** che, dapprima elaborazione e trattamento meramente meccanico di dati a livello informatico, oggi caratterizza i *software* e gli elaboratori dotati di ***machine learning***, quale capacità di autoapprendimento e correzione della tecnologia in relazione funzionale agli obiettivi in essa fissati.

Inoltre, i nuovi sistemi informatici e telematici si contraddistinguono per la relativa **connettività**, che favorisce attività di raccolta, elaborazione e scambio di dati di ogni dimensione, con la costante espansione di reti e strumenti di comunicazione e il crescente aumento degli utenti nella rete, al punto da determinare la costruzione del ***cyberspace***, quale infosfera virtuale, parallela alla realtà materiale e sensibile.

Il nuovo **spazio cibernetico** – così definito dalla scienza che studia le modalità e i mezzi attraverso cui l'essere umano e le nuove tecnologie trasmettono informazioni fra loro e con l'ambiente circostante – ha assunto una **dimensione sempre più globale, istantanea e immanente all'ordinamento**, al punto da superare il mondo del *web* e dell'*Internet of things* fino a divenire un elemento inscindibile rispetto alla realtà materiale contemporanea, tale da fondersi con quest'ultima nel complesso dinamismo evolutivo della società.

Allora, guardando alle ripercussioni in territorio penale, il progresso scientifico in ambito informatico e cibernetico ha prodotto, con la capillare diffusione dei sistemi tecnologici, oltre ai tradizionali ***computer crimes*** (o reati *informatici*, ai quali rinviava la **Raccomandazione emessa dal Consiglio d'Europa nel 1989**), la nuova categoria dei ***cybercrimes*** (i reati c.d. *cibernetici*) introdotti dalle previsioni in materia di diritto penale sostanziale e processuale della **Convenzione *Cybercrime* adottata a Budapest dal Consiglio d'Europa il 23 novembre 2001**, quale primo strumento internazionale vincolante per la lotta alla criminalità informatica.

Pertanto, oltre ai crimini che possono definirsi strettamente informatici – poiché comprensivi, fra i propri elementi tipizzati nella norma incriminatrice, dei concetti di sistema informatico, dato informatico, programma informatico e telematico, etc. –, l'insieme dei *cybercrimes* ha oggi assunto un significato tanto maggiore quanto quello dell'espansione del *cyberspace*, nonché tale da includervi qualsiasi reato venga perpetrato nella dimensione virtuale.

In buona sostanza, i reati cibernetici incriminano tutti quei comportamenti che consistono nella comunicazione e nella diffusione in rete di contenuti penalmente rilevanti (come la **diffamazione a mezzo *web*** e i **delitti di pedopornografia telematica**), che si caratterizzano per una notevole semplicità nell'attuazione e per gli effetti gravemente pregiudizievoli che, a causa della ricondivisione da parte di soggetti terzi, spesso sfuggono al controllo dell'autore che ha immesso per primo in rete il contenuto lesivo.

A tal riguardo, dunque, assumono rilievo nuove ipotesi di reato e nuove circostanze aggravanti, che nel tempo sono state recepite dall'ordinamento per introdurre trattamenti sanzionatori specificamente rivolti ad impedire nuove modalità di condotte criminose, come **il *cyberstalking*, la diffusione illecita di immagini o video sessualmente espliciti** (il c.d. *revenge porn*), **il *cyber*-bullismo** e via dicendo: dinanzi a questa molteplicità di reati, è divenuta imprescindibile la tutela apprestata dal legislatore alle nuove forme di criminalità informatica, in ragione del carattere potenzialmente senza limite della replicazione lesiva ai danni dell'interesse meritevole di protezione, oltreché della dimensione aperta e sconfinata di autori di reato e persone offese.

La pervasiva e crescente esposizione della società ai nuovi prototipi di ***Artificial Intelligence*** (*AI*) ha poi costretto il giurista ad una nuova riflessione, portandolo ad interrogarsi attorno alla necessità di integrare gli istituti tradizionali del diritto penale quale alternativa all'idea di ritenerlo un *arnese vecchio* per dare vita ad un nuovo quadro giuridico che si allontani dagli estremi del cardine costituzionale della **personalità della responsabilità penale** (art. 27, co. 1° Cost.).

Anche l'ordinamento nazionale, pertanto, a seguito del **regolamento (UE) 2024/1689** (c.d. *EU Artificial Intelligence Act*), ha mosso i primi passi nel campo del graduale riconoscimento dell'intelligenza artificiale in ambito penale, pur deponendo a favore della sua qualificazione quale strumento (e non autore diretto) del reato: il primo riferimento è al **disegno di legge n° 1146/2024**, predisposto per disciplinare l'utilizzo dei nuovi sistemi intelligenti nel rispetto dei principi di trasparenza, controllo umano e limiti settoriali per sanità e disabilità, lavoro, diritto d'autore, giustizia e Pubblica Amministrazione.

In materia penale, il testo normativo in corso di approvazione, anzitutto, ha introdotto una nuova **circostanza aggravante comune** per i reati realizzati mediante l'utilizzo dell'*AI* e una **circostanza aggravante ad effetto speciale** per i reati commessi contro i diritti politici del cittadino, quando perpetrati attraverso i nuovi sistemi tecnologici intelligenti; in secondo luogo, la bozza della novella ha previsto altresì l'introduzione del **delitto di illecita diffusione di contenuti generati o manipolati artificialmente** (noto anche come reato di *deepfake*) con la disposizione di cui all'**art. 612-*quater* c.p.**, che incrimina chiunque cagioni 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 manipolati attraverso l'utilizzo di sistemi di intelligenza artificiale, in grado di indurre in inganno sulla relativa genuinità o provenienza.

La punibilità di tali comportamenti, in breve, consentirà l'emersione di fenomeni come il *cyberstalking* e il *cyber*-bullismo, che molto spesso affliggono **soggetti vulnerabili** – anche di minore età – sottoposti a **trattamenti persecutori e lesivi della propria libertà personale** a causa della portata pregiudizievole di contenuti falsi (come audio, immagini e video) creati per esercitare attraverso la dimensione informatica e telematica forme di pressione, oltreché per aggredire, molestare, ricattare, denigrare, rubare l'identità, alterare e manipolare illecitamente dati sensibili a danno di particolari categorie di soggetti, ingiustamente colpiti dalla diffusione massiva di tali contenuti a una moltitudine indeterminata e indeterminabile di utenti del *web,* ivi comprese le persone vicine alle stesse vittime.

Ebbene, non sono pochi i casi in cui l'utilizzo distorto dell'intelligenza artificiale possa generare **contenuti identificabili come *deepfake*** che, già oggi, condurrebbero alla configurazione di reati come minacce, *revenge porn*, *stalking* e trattamento illecito di dati, ipotesi criminose cui sovente si ricorre per perseguire i fenomeni di *cyber*-bullismo riconosciuti dalla **legge 17 maggio 2024, n° 70** e, già prima, dalla **legge 29 maggio 2017, n° 71**.

Questi campi appaiono oggi del tutto in divenire per l'esperto di diritto, sempre più chiamato alla riflessione attorno alla materia della criminalità informatica e dei *cybercrimes* recepiti dalla normativa penale la quale, di pari passo con il progresso della scienza e della tecnica, deve saper cogliere l'andamento della società per il puntuale riconoscimento giuridico di fattispecie che impediscano pericolose lacune normative a presidio di **beni giuridici costituzionalmente garantiti**.