DIRITTO PENALE
E UOMO
Criminal Law and Human Condition

Articolo

Brevi note "a caldo" sulla recente Proposta di Regolamento UE in tema di intelligenza artificiale

The recent Proposal of the European Commission for a Regulation laying down harmonised rules on artificial intelligence: an overview

di Federico Carmelo La Vattiata

Abstract. *Il 21 aprile 2021, all'esito di un articolato processo normativo iniziato tre anni prima, la Commissione europea ha reso pubblica una Proposta di Regolamento, indirizzata al Parlamento europeo e al Consiglio,* «laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts».
La Proposta – attraverso «a proportionate and risk-based European regulatory approach» *– mira a realizzare due "obiettivi gemelli": affrontare il problema della gestione dei rischi associati a specifiche applicazioni di IA, promuovendo, nondimeno, la diffusione di tale tecnologia.*
Il presente contributo offre una prima lettura del documento, evidenziando, in particolare, i principali profili di interesse per il diritto penale sostanziale e processuale. Al riguardo, vengono individuate tre aree tematiche: a) l'ambito di rilevanza della Proposta e la definizione di IA; b) talune pratiche oggetto di divieto; c) le questioni relative al c.d. danno da prodotto intelligente.

Abstract. *On the 21st of April 2021, the European Commission published a Proposal for a Regulation of the European Parliament and of the Council «laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts». The package is the outcome of three years of intense policymaking on AI at European level.*
The Proposal – through «a proportionate and risk-based European regulatory approach» – pursues the "twin objectives" of addressing the risks associated with specific AI applications in a proportionate manner and of promoting the uptake of AI.

This article aims at providing an overview of the document. In particular, the main elements of interest for substantive criminal law and criminal procedure will be investigated. In this regard, they will be classified into three thematic areas: a) the scope of the Proposal and the definition of AI; b) the prohibited AI practices; c) the questions concerning the topic of ("intelligent") product liability.

1. Introduzione.

Il 21 aprile 2021 la Commissione europea ha reso pubblica una Proposta di Regolamento, indirizzata al Parlamento europeo e al Consiglio, «*laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*»[1] (di seguito "la Proposta"), in ordine alla quale, con queste brevi note, si intende fornire una prima lettura, con particolare attenzione ai profili di interesse dal punto di vista del diritto penale sostanziale e processuale.

Una lettura, questa, che inevitabilmente interviene "a caldo", per due ordini di ragioni: in primo luogo perché la pubblicazione del documento è avvenuta in tempi recentissimi; e in secondo luogo, perché le implicazioni per il diritto penale di un fenomeno tanto vasto, complesso e proteiforme meriterebbero, a ben vedere, ben più attente e ponderate considerazioni "a freddo", che nondimeno ci si riserva di produrre in altra occasione.

Invero, se pure sul piano teoretico è auspicabile che la riflessione penalistica italiana continui a scandagliare – con la pazienza propria dello studioso – le implicazioni suddette, si avverte altresì la necessità di offrire, senza indugio, una prima guida alla lettura del documento in oggetto, a favore anzitutto degli operatori del diritto lettori di questa Rivista. A quest'ultima va infatti riconosciuto il pregio di valorizzare, a seconda dei casi,

[1] COM(2021) 206 final.

non solo le esigenze legate alla ricerca scientifica, ma altresì quelle pratico-divulgative, in relazione a temi di scottante attualità.

Del resto, da una diversa e più generale prospettiva, le logiche della "ragion pura" e quelle della "ragion pratica" non necessariamente risultano inconciliabili; piuttosto, è stato efficacemente messo in luce come il compito precipuo della dogmatica consista proprio nel «mettere in comunicazione teoria e prassi»[2].

Va in ogni caso sottolineato, "stemperando" in qualche modo l'urgenza del commento, che si tratta pur sempre di una Proposta – per quanto autorevole – di Regolamento, la quale, nell'*iter* normativo che seguirà, potrà subire modifiche o, addirittura, arenarsi.

Comunque sia di ciò, nell'eventualità dell'entrata in vigore del testo in parola, *quid iuris* sotto il profilo specificamente penalistico?

2. La Comunicazione della Commissione europea «*Fostering a European approach to Artificial Intelligence*».

Dalla lettura del titolo («*laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*»)[3] si può intuire la finalità perseguita dalla Proposta, vieppiù specificata e argomentata, oltre che alla luce delle singole disposizioni della stessa, anche attraverso due ulteriori documenti, la cui lettura risulta conseguentemente indispensabile, al fine di cogliere il senso complessivo dell'operazione di politica del diritto inaugurata dalla Commissione.

In particolare, si tratta dell'*Explanatory Memorandum* introduttivo rispetto al testo della Proposta, e della Comunicazione (pubblicata nella medesima data) rivolta al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni, e intitolata "*Fostering a European approach to Artificial Intelligence*" (di seguito "la Comunicazione")[4].

Occorre prendere le mosse da quest'ultima.

In essa, la Commissione effettua anzitutto una ricognizione dei documenti in materia di intelligenza artificiale adottati dalle Istituzioni dell'Unione negli ultimi tre anni: la *Strategia europea sull'IA* (aprile 2018); le *Linee-guida per un'IA affidabile* (aprile 2019) e l'*Assessment List per l'IA affidabile* elaborate dal Gruppo di esperti di alto livello sull'IA nominato proprio dalla Commissione ("HLEG"); la creazione della *AI Alliance*, una piattaforma ideata col fine di consentire ad oltre quattromila *stakeholders* di dibattere sulle implicazioni tecnologiche e sociali dell'IA; un primo *Piano coordinato sull'IA* pubblicato nel dicembre 2018; il *Libro bianco della Commissione sull'IA*, pubblicato nel febbraio 2020

[2] S. Fiore, *La teoria generale del reato alla prova del processo: spunti per una ricostruzione integrata del sistema penale*, ESI, 2007, p. 184.
[3] Trad. it.: «che stabilisce regole armonizzate in tema di intelligenza artificiale (*Artificial Intelligence Act*) e che modifica taluni atti legislativi dell'Unione».
[4] COM(2021) 205 final.

insieme a un *report* in materia di sicurezza e responsabilità in relazione all'IA, all'*Internet of Things* (IoT) e alla robotica; e, infine, la consultazione pubblica sull'anzidetto *Libro bianco* che ha avuto luogo da febbraio a giugno 2020.

Breve: la Proposta rappresenta il punto di approdo di un processo normativo lungo tre anni[5].

Successivamente, viene rimarcato un profilo emerso già nel testo del citato *Libro bianco*. Invero, l'uso di tecnologie di IA comporta la produzione di una serie di rischi specifici, che il diritto vigente non è in grado di gestire. Sebbene sia infatti vero che, *de iure condito*, tanto a livello sovranazionale quanto a livello nazionale, vi siano solidi strumenti normativi idonei a proteggere i diritti fondamentali e a garantire la sicurezza dei consumatori, talune caratteristiche dell'IA potrebbero ostacolare l'applicazione e l'*enforcement* di tali strumenti.

Emergono quindi gli **obiettivi gemelli** della Proposta: affrontare il problema della gestione dei rischi associati a specifiche applicazioni di IA, promuovendo, nondimeno, la diffusione di tale tecnologia[6].

La realizzazione di un così ambizioso (duplice) obiettivo impone un approccio ispirato alla tecnica del bilanciamento di interessi e al principio di proporzione, onde predisporre un *corpus* normativo «*future-proof and innovation-friendly*»[7]: l'intervento regolatore, in altre parole, deve intervenire solo laddove e nella misura in cui sia strettamente necessario, minimizzando, ove possibile, i *costi* per gli operatori economici[8].

Alla luce di ciò, la Proposta è stata costruita su sette elementi che, complessivamente considerati, individuano «*a proportionate and risk-based European regulatory approach*»[9]:

i. una definizione di IA **tecnologicamente neutra**, in grado cioè di resistere alle istanze di mutamento imposte dalle continue evoluzioni tecnico-scientifiche nel settore;
ii. l'attenzione ai soli casi di impiego dell'IA *high-risk*, evitando in tal modo fenomeni di *over-regulation*;

---

[5] Così il testo della Comunicazione, cit., p. 5: «*The package published todayi s the outcome of 3 years of intense policymaking on AI at European level*» (trad. it.: «il complesso [di norme, n.d.a.] pubblicato in data odierna rappresenta il risultato di un processo normativo in materia di IA a livello europeo lungo tre anni»).
[6] Comunicazione, cit., p. 6.
[7] *Ibidem* (trad. it.: «in grado di resistere ai mutamenti socio-tecnologici e attento alla innovazione»).
[8] Trad. it.: «un approccio regolatorio improntato al principio di proporzione e alla valutazione del rischio».
È evidente, qui, l'incidenza dell'analisi economica del diritto. Sul tema si rinvia *ex multis* alle seguenti fondamentali opere: R.H. Coase, *The Firm, the Market, and the Law*, University of Chicago Press, 2004;G. Calabresi, *First Party, Third Party, and Product Liability Systems: Can Economic Analysis of Law Tell Us Anything About Them?*, in *Iowa Law Review*, 69, 1984, pp. 833 ss.; R.A. Posner, *Economic Analysis of Law,* 9ª ed., Wolters Kluwer, 2014.
Per un'analisi recente (ancorché focalizzata sul particolare settore della criminalità legata alla tossicodipendenza) in tema di analisi economica del diritto penale, si veda F. Pesce, *L'analisi economica del diritto penale dalla teoria alla pratica. Il livello di efficienza delle opzioni normative in tema di tossicodipendenza e criminalità correlata*, Editoriale Scientifica, 2019.
[9] Comunicazione, cit., pp. 6 ss.

iii. l'individuazione di taluni requisiti specifici che i sistemi di IA ad alto rischio devono rispettare per poter superare un *test* di conformità prodromico alla immissione sul mercato o alla messa in servizio;
iv. l'introduzione di un divieto relativo ad alcuni usi dell'IA, tassativamente identificati, giustificato dall'elevato rischio di lesione dei valori dell'Unione e dei diritti fondamentali;
v. l'adozione di un approccio particolarmente restrittivo con riguardo ai sistemi di identificazione biometrica da remoto (ad esempio, strumenti di riconoscimento facciale)[10];
vi. la previsione di requisiti di trasparenza algoritmica minimi per i sistemi IA non ad alto rischio (ad esempio, *chatbots*);
vii. infine, la previsione di incentivi all'uso di *regulatory sandboxes* (*i.e.* spazi di sperimentazione normativa)[11], al fine di testare tecnologie innovative per un periodo di tempo limitato, nonché accedere a *Digital Innovation Hubs* e a servizi per il test e la sperimentazione dei sistemi.

Breve: l'obiettivo **bifronte** della Proposta consiste nella protezione dei diritti fondamentali, cruciale per la realizzazione di una *trustworthy AI*, senza con ciò inibire il profilo, parimenti importante, dell'innovazione tecnologica, la quale, però, dev'essere *umanocentrica* («*human-centric*»)[12].

3. La Proposta di Regolamento «*Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*».

*3.1. L'*Explanatory Memorandum.

Come anticipato, la Proposta di Regolamento è corredata di un *Explanatory Memorandum*,che, oltre a riprodurre in larga parte le considerazioni contenute nella Comunicazione (v. *supra*, § 2), funge da introduzione al documento, specificandone alcuni profili.

La premessa, per dir così epistemologica, dell'iniziativa legislativa della Commissione è rappresentata da un aspetto ampiamente scandagliato dai documenti prodotti in precedenza dalle Istituzioni. Invero, l'IA è suscettibile di apportare certamente numerosi benefici dal punto di vista sociale ed economico, attraverso un miglioramento delle predizioni, l'ottimizzazione delle operazioni e della allocazione di risorse, nonché

[10] Segnatamente, l'applicazione di simili sistemi per finalità di *law enforcement* deve ritenersi in linea di principio vietata negli spazi accessibili pubblicamente, salvo eccezionali disposizioni di legge di autorizzazione (comunque soggette a talune salvaguardie). Inoltre, tutti i sistemi di riconoscimento facciale devono essere sottoposti a una procedura *ex ante* di valutazione di conformità da parte di un ente certificatore terzo, nonché a più rigorosi requisiti di *logging* e controllo umano.
[11] Sul tema v. Consiglio dell'Unione europea, *Conclusioni sugli spazi di sperimentazione normativa e le clausole di sperimentazione come strumenti per un quadro normativo favorevole all'innovazione, adeguato alle esigenze future e resiliente che sia in grado di affrontare le sfide epocali nell'era digitale*, 13026/20, 16 novembre 2020; nonché R. Parenti, *Regulatory Sandboxes and Innovation Hubs for FinTech. Impact on innovation, financial stability and supervisory convergence – Study for the committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament*, 24 settembre2020.
[12] Comunicazione, cit., p. 1.

personalizzando i servizi di *delivery*. Tuttavia, è altresì idonea a produrre nuovi rischi per i diritti e i valori tutelati dal diritto dell'Unione[13].

Ne consegue la necessità di un intervento normativo in grado di massimizzare i benefici riducendo i rischi e, in particolare, mirato alla realizzazione dei seguenti obiettivi specifici:

i. assicurare che i sistemi di IA immessi sul mercato unico e ivi impiegati siano sicuri e applicati nel rispetto dei diritti fondamentali e dei valori dell'Unione;
ii. assicurare la certezza del diritto, così da incentivare gli investimenti e l'innovazione nel settore;
iii. rendere più efficiente l'applicazione di quelle regole, già in vigore, sotto il cui ombrello applicativo sono destinati a ricadere taluni sistemi di IA;
iv. creare in ultima analisi le fondamenta per lo sviluppo di un mercato unico delle applicazioni di IA, improntato ai valori della legalità, della sicurezza e della fiducia.

Viene quindi esplicitato un profilo rilevantissimo: il proposto sistema di regole armonizzate riguarda, alla stregua di un *proportionate risk-based approach*, tutte e tre le fasi della vita dei sistemi IA, *i.e.* lo sviluppo, l'immissione nel circuito economico, nonché la loro concreta applicazione.

Senonché, un primo problema, ben chiaro alla Commissione, e che dovrà essere affrontato dagli interpreti, attiene al rapporto tra le disposizioni del nascente Regolamento e il diritto dell'Unione già in vigore, disciplinante settori economici nevralgici in cui i sistemi di IA ad alto rischio sono già applicati (o verosimilmente lo saranno in tempi brevi). Da questo punto di vista, viene in considerazione la possibilità che i sistemi in parola costituiscano componenti di prodotti, il cui ciclo di sviluppo e applicazione risulti già disciplinato dal diritto sovranazionale. Occorrerà allora procedere a delicate operazioni ermeneutiche, al fine di assicurare coerenza normativa, evitare duplicazioni e minimizzare i costi addizionali per gli operatori economici.

Ebbene, con riguardo ai prodotti rientranti nel campo di applicazione *rationemateriae* della c.d. *New Legislative Framework* (NLF) *legislation* (ad esempio, macchinari, dispositivi medici, giocattoli, etc.)[14], i requisiti previsti dalla Proposta per i sistemi di IA ad alto rischio si aggiungeranno a quelli già previsti dalla normativa di settore, contribuendo a formare il parametro delle relative procedure di valutazione di conformità. In particolare, nell'ottica di tale reciproca compenetrazione normativa («*the interplay of requirements*»), mentre la Proposta fa riferimento a requisiti il cui rispetto viene ritenuto in

[13] In argomento v. *ex multis* C. Casonato, *Potenzialità e sfide dell'intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, Fasc. 1, 2019, pp. 177 ss.; Id., *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, in *BioLaw Journal – Rivista di BioDiritto*, Fasc. 2, 2019, pp. 711 ss.;S. Quattroccolo, *Equo processo penale e sfide della società algoritmica*, in *BioLaw Journal – Rivista di BioDiritto*, Fasc. 1, 2019, pp. 135 ss.; S. Riondato, *Robot: talune implicazioni di diritto penale*, in *Tecnodiritto: temi e problemi di informatica e robotica giuridica* (a cura di)P. Moro, C. Sarra, Milano, Franco Angeli, 2017, pp. 85 ss.; B. Caravita di Torrito, *Principi costituzionali e intelligenza artificiale*, in U. Ruffolo, (a cura di), in*telligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, 2020, pp. 451 ss.;P. Severino, *Intelligenza artificiale e diritto penale*, in *ivi,* pp. 531 ss.; V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *ivi,*pp. 547 ss.; A. Amidei, *La* governance *dell'Intelligenza Artificiale: profili e prospettive di diritto dell'Unione Europea*, in *ivi*, pp. 571 ss.
[14]Cfr. https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en.

grado di assicurare una equilibrata gestione dei rischi specifici posti dai sistemi di IA, le norme della legislazione NLF garantiscono la sicurezza complessiva del prodotto finale.

Breve: la normativa di settore potrebbe prevedere requisiti ulteriori rispetto a quelli di cui alla Proposta, attinenti alla integrazione in sicurezza di un sistema IA all'interno di una classe più ampia di prodotti[15].

Vengono poi in considerazione i criteri di scelta dello strumento normativo e l'individuazione della relativa base giuridica.

La scelta dello strumento regolamentare (in luogo, per esempio, di una direttiva, com'è noto meno incisiva dal punto di vista dell'armonizzazione normativa) si giustifica alla luce dell'esigenza di uniformare l'applicazione di regole nuove tra gli Stati membri, individuando la base giuridica per l'adozione di tale strumento, anzitutto, nell'art. 114 TFUE, il quale prevede l'adozione di misure idonee ad assicurare l'istituzione e il funzionamento del mercato interno e, in subordine, con riferimento alle regole in materia di protezione dei dati personali, nell'art. 16 TFUE.

Sono inoltre importanti i rilievi in tema di rispetto dei principi di sussidiarietà e proporzione.

Sotto il primo profilo, viene sottolineata la natura ormai "ubiquitaria" dell'IA, destinata ad essere integrata in un numero sempre crescente di prodotti e servizi, a loro volta destinati a circolare liberamente nell'Unione. Sarebbe pertanto irrealistico perseguire gli obiettivi prefissati (cfr. *retro*) attraverso strumenti normativi meno penetranti rispetto al regolamento.

Sotto il secondo profilo, occorre distinguere a seconda che i sistemi di IA siano ad alto rischio oppure no: nel primo caso, la Proposta individua solo quei requisiti ritenuti indispensabili al fine di mitigare i rischi per i diritti fondamentali e i valori dell'Unione (che non possono essere protetti attraverso i vigenti strumenti normativi); peraltro, ove non *high-risk*, il sistema deve rispettare alcuni più blandi requisiti di trasparenza algoritmica.

Particolare rilievo assume l'attenzione per i *Grundrechte*.

Sul punto, la Commissione si dimostra ben consapevole di introdurre significative restrizioni alla libertà di iniziativa economica e alla libertà artistica e scientifica, rispettivamente protette dagli articoli 16 e 13 della Carta di Nizza. Nondimeno, tale sacrificio viene ritenuto indispensabile e giustificato, secondo una logica di bilanciamento, al fine di garantire diritti e libertà, parimenti fondamentali, considerati prevalenti (anzitutto la salute, la sicurezza e la protezione dei consumatori).

Breve: (anche) l'innovazione tecnico-scientifica deve essere *responsabile*, *i.e.* rispettosa dei diritti fondamentali e dei valori dell'Unione.

[15] V. altresì il Considerando n. 63.

3.2. La Proposta: alcune possibili implicazioni per il diritto penale.

Veniamo adesso a passare in rassegna l'architettura complessiva del documento.

La Proposta è strutturata in dodici titoli. Questi – secondo l'*Explanatory Memorandum* – possono essere classificati secondo un criterio di ordine tematico. Ne risultano otto gruppi di disposizioni, rispettivamente dedicati:

i. all'ambito applicativo della Proposta e alle norme definitorie (titolo I);
ii. alle pratiche oggetto di divieto (titolo II);
iii. ai sistemi di IA qualificabili come ad alto rischio (titolo III)
iv. ai requisiti di trasparenza richiesti per talune classi di sistemi IA (titolo IV);
v. alle misure di incentivazione dell'innovazione (titolo V);
vi. ai sistemi di *governance* e all'implementazione delle norme di cui alla Proposta (titoli VI, VII e VIII);
vii. ai codici di condotta (titolo IX); e
viii. alle disposizioni di chiusura (titoli X, XI e XII).

In particolare, dal punto di vista penalistico, sono tre le aree di interesse individuabili alla luce di una lettura globale della Proposta: l'enucleazione di una definizione di IA; il divieto *tout court* di talune pratiche;le questioni relative al tema del c.d. danno daprodotto intelligente.

3.2.1. Il campo di applicazione della Proposta e la definizione di IA.

Sotto il primo profilo, l'art. 2 circoscrive il campo d'applicazione *ratione personae*: i *providers*[16] che immettono sul mercato o mettono in servizio sistemi di IA all'interno dell'Unione, indipendentemente dal fatto che essi abbiano o meno la propria sede nel territorio UE ovvero in uno Stato terzo; gli *users*[17] di sistemi di IA collocati nell'Unione; i *providers* e gli utenti di sistemi che, pur non sviluppati/prodotti all'interno dell'Unione, generino un *output* impiegato nell'UE (par. 1).

Peraltro, viene specificato che il Regolamento non si applicherà ai sistemi sviluppati o impiegati esclusivamente a fini militari, né alle autorità pubbliche di uno Stato terzo o alle organizzazioni internazionali, laddove tali soggetti impieghino i sistemi IA nel quadro di accordi internazionali con finalità di *law enforcement*[18] e di cooperazione giudiziaria con l'Unione o con gli Stati membri (par. 3 e 4).

Per quanto concerne poi l'enucleazione della nozione di IA ai fini del Regolamento, sotto il profilo della certezza giuridica, è particolarmente apprezzabile lo sforzo definitorio,

[16] Per *provider* si intende una persona fisica o giuridica, un'autorità pubblica, un'agenzia o altro ente che sviluppi o abbia sviluppato un sistema di IA nell'ottica di una sua immissione sul mercato o messa in servizio in nome proprio, sia a pagamento che gratuitamente (art. 3 par. 2).
[17] Per *user* si intende una persona fisica o giuridica, un'autorità pubblica, un'agenzia o altro ente che faccia uso di un sistema di IA sotto la propria responsabilità, salvo i casi in cui tale sistema sia impiegato nel corso di un'attività personale non professionale.
[18] Ai sensi dell'art. 3 par. 41, per *law enforcement* si intende ogni attività indirizzata alla prevenzione, all'indagine alla scoperta e alla prosecuzione di reati ovvero all'esecuzione delle sanzioni penali.

alla luce dell'assenza, all'interno della comunità scientifica, di una nozione univocamente accreditata[19].

Un obiettivo, quello della **certezza**, evidenziato dal Considerando n. 6, il cui testo tiene altresì conto dell'opposta esigenza di **elasticità** concettuale, così da consentire la copertura di eventuali sviluppi tecnologici futuri.

Conseguentemente, la nozione di IA viene costruita, come sarà chiarito a breve, attorno alle caratteristiche funzionali fondamentali del *software*, considerando, tra le altre cose, per un verso, i variabili livelli di **autonomia** che un sistema può presentare e, per altro verso, la possibilità che esso sia impiegato come dispositivo *stand-alone*, ovvero come componente di un più complesso prodotto, a prescindere dalla sua fisica integrazione in esso (*i.e.* rilevano sia i sistemi c.d. *embedded*, sia quelli c.d. *non-embedded*).

L'art. 3 par. 1 afferma che, ai fini del Regolamento, per **sistema di intelligenzaartificiale** (o **sistema IA**) si intende un *software* sviluppato con una tecnica o un approccio tra quelli elencati nell'Allegato I[20] e che, per una certa gamma di obiettivi definiti da un essere umano, sia in grado di generare *outputs* – quali contenuti, predizioni, consigli, ovvero decisioni – idonei ad influenzare l'**ambiente** col quale tale sistema interagisce.

3.3.2. Talune pratiche oggetto di divieto e in particolare l'uso di sistemi di identificazione biometrica da remoto "*real-time*" in spazi accessibili al pubblico e per finalità di *law enforcement*.

L'art. 5 individua talune pratiche dotate, secondo un calcolo rischi-benefici, di idoneità lesiva tale da giustificare la previsione di un divieto.

Tra queste, rileva soprattutto l'uso con finalità di *law enforcement*, in spazi accessibili al pubblico, di sistemi di identificazione biometrica da remoto "*real-time*", ossia sistemi in base ai quali la raccolta, la comparazione e l'individuazione dei dati biometrici

[19] In argomento, v. S.J. Russell, P. Norvig, *Artificial Intelligence. A Modern Approach*, 4ª ed., Pearson, 2021, pp. 1 ss.

[20] Segnatamente: approcci di *machine learning* (o "ML"), tra cui il *supervised*, l'*unsupervised* e il *reinforcement learning*, che applicano vari metodi, e.g. il *deep learning* (o "DL"); approcci c.d. *knowledge-based* o *logic-based*, come le rappresentazioni, la programmazione induttiva e i sistemi esperti; nonché approcci statistici, valutazioni bayesiane e metodi di ricerca e ottimizzazione.
Per ulteriori dettagli tecnici su ciascuno di questi metodi o approcci, v. *amplius*, S.J. Russell, P. Norvig, *Artificial Intelligence*, cit.
Qui basterà rammentare sinteticamente la più generale definizione data dalla stessa Commissione europea nella sua Comunicazione *Artificial Intelligence for Europe* del 25 aprile 2018 [COM(2018) 237 final], e richiamata da F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *questa rivista*, 10, 2019, 1 ss.: «l'intelligenza artificiale (IA) indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi. I sistemi basati sull'IA possono consistere solo in *software* che agiscono nel mondo virtuale (ad esempio, assistenti vocali, *software* per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale), oppure incorporare l'IA in dispositivi *hardware* (ad esempio, in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle Cose)».

avviene senza apprezzabile soluzione di continuità[21], fatti salvi, peraltro, i casi in cui tale uso risulti **strettamente necessario** per il perseguimento di tre **finalità specifiche**:

i. la ricerca mirata di potenziali vittime di reato;
ii. la prevenzione di **specifiche**, **sostanziali** e **imminenti** minacce alla vita o all'integrità fisica delle persone, ovvero la prevenzione di attacchi terroristici;
iii. la cattura, la localizzazione, l'identificazione o la prosecuzione di autori (o supposti tali) di uno tra i reati di cui all'art. 2 par. 2 della Decisione quadro 2002/584/GAI in materia di **mandato d'arresto europeo**.

L'impiego dei sistemi in commento dovrebbe avvenire tenendo in considerazione, da un lato, la serietà, la probabilità e l'intensità dell'eventuale danno causato dalla loro mancata applicazione, ma altresì, dall'altro, le conseguenze, potenzialmente derivanti dal loro uso, per i diritti e le libertà di tutte le persone coinvolte. A tal proposito, è necessario che l'impiego di tali sistemi sia limitato sia *ratione temporis*, sia *ratione loci*, sia *ratione personae*. Inoltre, occorre una previa autorizzazione da parte dell'Autorità giudiziaria ovvero di un'Autorità amministrativa indipendente dello Stato membro, emessa a seguito di richiesta motivata e nel rispetto di regole nazionali **dettagliate** che limitino l'esercizio di un potere tanto invasivo e impattante su beni giuridici supremi. Detta autorizzazione potrà essere rilasciata solo laddove siano accertate, sulla base di prove oggettive e di chiare indicazioni tanto l'**assoluta necessità**, quanto la **proporzionalità** dell'uso dei sistemi in parola, in relazione ad almeno uno degli obiettivi suddetti, da indicare specificamente nella richiesta di emissione.

3.3.3. Alcuni profili rilevanti in tema di danno da prodotto intelligente.

In terzo luogo, vengono in considerazione taluni profili riconducibili alla tematica, di per sé complessa, del c.d. **danno da prodotto**.

Su questo terreno si coglie, con estrema evidenza, la problematicità del fenomeno che la Proposta mira a regolare.

Com'è stato già sottolineato, infatti, le tecniche di IA sono tanto foriere di grandi benefici per la società[22], quanto dotate di una spiccata idoneità lesiva con riferimento a una ridda di beni giuridici fondamentali (*in primis* la vita, la salute e la sicurezza degli individui)[23].

Proprio sulla base di tale constatazione, adottando un approccio *risk-based*, la Commissione non si è limitata all'introduzione di un divieto (nella sostanza ispirato al principio di **precauzione**)[24] concernente talune pratiche ritenute così rischiose per i

[21] Art. 3 par. 37.
[22] Considerando n. 3.
[23] Considerando n. 4.
[24] In materia di rapporti tra principio di precauzione e diritto penale, v. *ex multis* M. Donini, *Un nuovo medioevo penale? Vecchio e nuovo nell'espansione del diritto penale economico*, in *Cass. Pen.*, 6, 2003, pp. 1808 ss.; C. Piergallini, *Danno da prodotto e responsabilità penale. Profili dommatici e politico-criminali*, Giuffrè, 2004; G. Forti, *"Accesso" alle informazioni sul rischio e responsabilità: una lettura del principio di precauzione*, in *Criminalia*, 2006, pp. 155 ss.; F. Giunta, *Il diritto penale e le suggestioni del principio di precauzione*, in *Criminalia*, 2006, pp. 227 ss.; D. Castronuovo, *Principio di precauzione e diritto penale. Paradigmi dell'incertezza nella*

Rechtsgüter da non poter essere in alcun modo ammesse, nemmeno prevedendo delle cautele.

Piuttosto, ha altresì individuato (essendo questo il *core* del complessivo impianto normativo) sia i requisiti che i sistemi di IA ad alto rischio devono possedere, sia i corrispondenti obblighi in capo agli operatori economici coinvolti nel loro ciclo di produzione e commercializzazione.

Infine, nel rispetto del principio di proporzione, ha valutato, con riferimento ad alcuni sistemi non ritenuti ad alto rischio, di introdurre degli obblighi di *trasparenza* meno rigorosi[25].

Alla luce del disposto dell'art. 6, possono essere individuate due classi di sistemi *high-risk*.

In primo luogo, se il sistema rientra tra quelli elencati nell'Allegato III, dev'essere considerato *in re ipsa*ad alto rischio. Vengono qui in considerazione i sistemi di identificazione biometrica e categorizzazione delle persone fisiche, nonché i diversi sistemi con finalità di *law enforcement*[26]. Con particolare riferimento a questi ultimi (*e.g.* sistemi di predizione della recidiva, sistemi di profilazione impiegati nel corso delle indagini preliminari, o sistemi di valutazione dell'affidabilità delle prove nel processo penale), appare evidente il potenziale sacrificio per il diritto a un ricorso effettivo[27], il diritto al *processo* equo[28], il diritto di difesa[29], così come per il principio della presunzione di innocenza[30], nei casi in cui il sistema non risulti sufficientemente trasparente, spiegabile, o non corredato di adeguata documentazione.

Un secondo criterio di attribuzione della qualifica *high-risk* consiste nella soddisfazione di almeno una delle seguenti condizioni: *a)* il sistema IA è destinato ad essere impiegato quale componente di sicurezza[31] di (ovvero è esso stesso) un prodotto

---

struttura del reato, Aracne, 2012; C. Brusco, *Rischio e pericolo, rischio consentito e principio di precauzione. La c.d. "flessibilizzazione delle categorie del reato"*, in *Criminalia*, 2012, pp. 391 ss.; E. Corn, *Il principio di precauzione nel diritto penale. Studio sui limiti all'anticipazione della tutela penale*, Giappichelli, 2013, pp.52 ss.; M. del Tufo, *Principio di precauzione e gestione del rischio: quali spazi applicativi per il diritto penale?*, in G. Carlizzi, G. Tuzet (a cura di), *La prova scientifica nel processo penale*, Giappichelli, 2018, pp. 137 ss.
Nella letteratura straniera, v. per tutti C.M. Romeo Casabona, *Aportaciones del principio de precaución al derechopenal*, in Id., *Principio de precaución, biotecnología y derecho*, Universidad de Deusto – Universidad de País Vasco – Comares, 2004, pp. 385 ss.

[25] Considerando n. 14

[26] Cfr. Considerando n. 38.

[27] Cfr. argomento v. D.P. Domenicucci, F. Filpo, *La tutela giurisdizionale effettiva nel diritto dell'Unione europea*, in S. Allegrezza, R. Mastroianni, O. Pollicino, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, 2017, pp.864 ss.; M. Caianiello, *Giudice imparziale precostituito e tutela effettiva dei diritti in materia penale*, in *ivi*, pp.903 ss.

[28] Si vedano le opere citate in nota 26.

[29] Cfr. S. Allegrezza, A. Mosna, *I diritti della difesa*, inS. Allegrezza, R. Mastroianni, O. Pollicino, O. Razzolini (a cura di), *Carta dei diritti fondamentali*, cit., pp.946 ss.

[30] Cfr. L. Luparia, J. della Torre, *La presunzione di innocenza*, inS. Allegrezza, R. Mastroianni, O. Pollicino, O. Razzolini (a cura di), *Carta dei diritti fondamentali*, cit., pp. 915 ss.

[31] Si tratta di «*a component of a product or of a system whichfulfils a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property*» (art. 2 par. 14) [trad. it.: «un componente di un prodotto o sistema che, per tale prodotto o sistema, integra una funzione di

rientrante nel campo di applicazione della normativa armonizzata di cui agli atti elencati nell'Allegato II (*e.g.* la Direttiva c.d. macchine CE/2006/42, o il Regolamento c.d. dispositivi medici UE/2017/745); *b)* il prodotto di cui il sistema IA è componente di sicurezza, ovvero il sistema IA stesso come prodotto, dev'essere sottoposto alla valutazione di conformità di un ente certificatore terzo prima di essere immesso sul mercato o messo in servizio, ove previsto dalla normativa armonizzata suddetta.

L'art. 8 consacra l'obbligatorietà dei requisiti previsti per i sistemi ad alto rischio. Requisiti, questi, che possono essere così compendiati:

i. i *datasets* impiegati per l'addestramento e la validazione dei sistemi devono rispondere a parametri di alta qualità (art. 10), affinché il loro rendimento sia sicuro e in linea con la destinazione d'uso, dovendo a questo riguardo consistere in dati, relativamente alla destinazione anzidetta, rilevanti, sufficientemente rappresentativi, immuni da errori e completi[32];
ii. occorre, prima di immettere un sistema nel circuito economico, predisporre la relativa documentazione tecnica, la quale deve dimostrare il rispetto dei requisiti di cui al Regolamento (art. 11)[33];
iii. è poi necessario che i sistemi siano programmati e sviluppati con caratteristiche tali da consentire, all'atto del loro impiego, la registrazione automatica degli eventi (c.d. *logs*), assicurando in tal guisala tracciabilitàdi funzionamento lungo tutto il loro ciclo di vita e, quindi, il monitoraggio delle operazioni, anche nell'ottica della c.d. *post-market surveillance* (art. 12)[34];
iv. ai sensi dell'art. 13, gli algoritmi impiegati dovranno essere *trasparenti*, in modo da consentire agli utenti l'interpretazione dell'*output* del sistema, e assicurare, pertanto, un uso corretto dello stesso; inoltre, ogni sistema dovrà essere corredato di una serie di istruzioni per l'uso concise, complete, corrette, chiare e formulate in termini comprensibili per gli *users* (informazioni, queste, che dovranno riguardare: il *provider* e/o un suo rappresentante; le caratteristiche, le capacità e i limiti del sistema; i cambiamenti attesi – pre-determinati – nel sistema e nel suo funzionamento; le misure di controllo umano, tra cui quelle di interpretazione dell'*output*; una stima della durata di funzionamento del sistema e ogni misura di manutenzione e cura, inclusi gli aggiornamenti)[35];
v. l'art. 14 prevede una serie di importantissimi requisiti riguardanti il controlloumano dei sistemi, *i.e.* questi dovranno essere programmati e sviluppati in modo tale da garantire, secondo modalità specificamente prescritte (v. *amplius* par. 4), il loro effettivo controllo da parte di una persona fisica all'atto dell'utilizzo, al dichiarato fine (par. 2) di prevenire o minimizzare i rischi per la salute, la sicurezza o i diritti fondamentali, che possono emergere in relazione sia alla destinazione d'uso, sia ai prevedibili usi impropri del *device*[36];

---

sicurezza, ovvero il cui fallimento o malfunzionamento mette a rischio la salute e la sicurezza delle persone o la proprietà»].
[32] V. *amplius* Considerando nn. 44 e 45.
[33] V. altresì Considerando n. 46.
[34] *Ibidem*.
[35] V. altresì Considerando n. 47.
[36] V. altresì Considerando n. 48.

vi. ai sensi dell'art. 15, i sistemi dovranno garantire un appropriato livello di precisione e c.d. robustezza (*i.e.* resilienza rispetto tanto alle limitazioni proprie del sistema – quali errori, fallimenti, situazioni impreviste o incongruenze – quanto ad eventuali azioni di compromissione della sua sicurezza); peraltro, con particolare riferimento ai sistemi c.d. dinamici, ossia quelli che continuano ad apprendere dopo lo sviluppo e la commercializzazione, occorrerà assicurare la possibilità di intervento su eventuali *output* affetti da *bias* attraverso puntuali misure correttive[37];

vii. infine, il par. 4 dell'art. 15 dispone in ordine alla c.d. *cybersecurity* dei sistemi, i quali, invero, attraverso misure di contrasto adeguate in relazione alle diverse classi di rischio, dovranno essere resilienti rispetto ai tentativi, da parte di terzi non autorizzati, di alterazione del loro utilizzo o della loro *performance* (ad esempio manipolazioni dei *training datasets*, ovvero la predisposizione intenzionale di *input* fallaci al fine di causare un errore del sistema)[38].

Così individuati gli obblighi relativi ai requisiti che un sistema ad alto rischio deve rispettare per poter essere immesso nel circuito economico, i successivi articoli 16-29 definiscono i campi personali di responsabilità per la loro osservanza.

A ben vedere, tali disposizioni definiscono l'ambito di rilevanza di taluni «poteri e doveri corrispondenti a dati ruoli»[39]. Esse, anche alla luce di quanto già emerso dalla lettura del documento, mirano a realizzare una forma rafforzata di protezione nei confronti di alcuni *Rechtsgüter* ritenuti fondamentali. A tal fine, vengono specificamente individuati i destinatari degli obblighi (non rivolti, dunque, alla generalità dei consociati)[40]. Ne consegue la nascita di quello «speciale vincolo di tutela»[41] tra beni e garanti proprio delle posizioni di garanzia, il quale consentirà, nei casi di ritenuta applicabilità di una compatibile fattispecie di parte speciale, l'operabilità del meccanismo di integrazione fondato sul combinato disposto tra tale fattispecie e l'art. 40 cpv c.p.[42].

Ebbene, gli obblighi in parola sono variamente, ma dettagliatamente, distribuiti tra le seguenti categorie di soggetti: *a)* il *provider* (artt. 16-23); *b)* i produttori (art. 24); *c)* i rappresentanti autorizzati dei *provider* non aventi sede nell'Unione, nel caso in cui non sia possibile identificare un importatore (art. 25); *d)* gli importatori di sistemi sviluppati fuori dall'UE (art. 26); *e)* i distributori (art. 27); e, infine, *f)* gli utenti (art. 29).

---

[37] V. altresì Considerando nn. 49-51.
[38] *Ibidem*.
[39] D. Pulitanò, *Diritto penale*, 8ª ed., Giappichelli, 2019, p.193.
[40] Si veda, vieppiù, il Considerando n. 53, ove viene enfatizzata la posizione del *provider*, destinatario principale, sia sotto il profilo quantitativo, sia sotto quello qualitativo, degli obblighi: «*It is appropriate that a* specific (enfasi aggiunta, n.d.a.) *natural or legal person, defined as the provider, takes the responsibility for the placing on the market or puttinginto service of a high-risk AI system, regardless of whethert hat natural or legal personis the person who designed or developed the system*» (trad. it.: «è opportuno che una specifica persona fisica o giuridica, definita come *provider*, assuma la responsabilità della immissione sul mercato o messa in servizio del sistema IA ad alto rischio, indipendentemente dal fatto che detta persona fisica o giuridica sia il progettista o lo sviluppatore del sistema»).
[41] Così G. Fiandaca, E. Musco, *Diritto penale. Parte generale*, 8ª ed., Zanichelli, 2019, pp. 650 ss.
[42] Sul tema, si vedano ampiamente *ex multis* F. Sgubbi, *Responsabilità penale per omesso impedimento dell'evento*, CEDAM, 1975; G. Fiandaca, *Il reato commissivo mediante omissione*, Giuffrè, 1979; G. Grasso, *Il reato omissivo improprio. La struttura obiettiva della fattispecie*, Giuffrè, 1983.

Rinviando per ulteriori dettagli al testo delle disposizioni testé richiamate, qui basterà riportare il quadro sintetico dei principali ambiti di responsabilità.

i. Ai sensi dell'art. 16[43], il *provider* è tenuto: in generale, a garantire il rispetto dei requisiti di cui agli artt. 8-14 (v. *retro*); a dotarsi di un sistema di gestione della qualità dei sistemi (v. *amplius* art. 17); a predisporre la loro documentazione tecnica; ad assicurare, prima dell'inserimento di tali sistemi nel circuito economico, il superamento della procedura di valutazione di conformità; ove trattasi di *stand-alone systems*, a registrarli, ai sensi dell'art. 51, nel *database* appositamente curato dalla Commissione con la collaborazione degli Stati membri; e, infine, a dotarsi di un adeguato sistema di monitoraggio post-commercializzazione dei sistemi.

ii. Laddove un sistema IA ad alto rischio costituisca il *safety component* di un prodotto rientrante nel campo di applicazione di un atto della *New Legislative Framework legislation* e non sia commercializzato indipendentemente da tale prodotto, il produttore di questo sarà responsabile della compatibilità del sistema con le norme del Regolamento, gravando su di esso gli obblighi propri del *provider* (art. 24 e Considerando n. 55).

iii. Nel caso in cui il sistema sia sviluppato fuori dall'Unione e non sia identificabile un importatore, i *provider* di Stati terzi dovranno, giusta delega scritta, individuare un rappresentante autorizzato nell'UE (art. 25 e Considerando n. 56).

iv. Sono poi previsti alcuni specifici obblighi a carico di importatori e distributori (art. 26 s. e Considerando n. 57). Segnatamente, gli importatori dovranno assicurare, prima dell'introduzione del sistema nel mercato unico: *a)* che il *provider* abbia effettuato la procedura di valutazione di conformità; *b)* che abbia altresì predisposto la documentazione tecnica; nonché *c)* che il sistema presenti il richiesto marchio di conformità, e sia corredato della documentazione tecnica e delle istruzioni per l'uso. I distributori dovranno verificare: *a)* l'etichettatura CE dei sistemi; *b)* la presenza della relativa documentazione; e *c)* che, a seconda dei casi, il *provider* o l'importatore abbia rispettato gli obblighi imposti dal Regolamento.

v. Infine, gli utenti dovranno: *a)* impiegare i sistemi conformemente a quanto disposto nelle istruzioni per l'uso e, in relazione a queste, monitorarne il funzionamento; *b)* nella misura in cui sia possibile controllare i dati *input*, assicurare la coerenza di questi rispetto alla destinazione d'uso dichiarata; e *c)* alla stregua delle informazioni ricevute ai sensi dell'art. 13 (v. *retro*), effettuare una valutazione d'impatto relativamente alla protezione dei dati personali, alla luce degli artt. 35 Regolamento UE/2016/679 e 27 Direttiva UE/2016/680.

È importante sottolineare, infine, come la valutazione di conformità dei sistemi segua una differente disciplina a seconda che essi siano o meno *high-risk*.

La regola generale è che, mentre per i secondi la valutazione dovrà essere effettuata direttamente dal *provider* sotto la propria responsabilità, per i primi occorrerà il coinvolgimento di un ente certificatore terzo.

[43] V. altresì Considerando n. 54.

Tuttavia, vi sono delle eccezioni.

Anzitutto, per i sistemi di identificazione biometrica delle persone fisiche, si dovrà sempre prevedere il coinvolgimento di un ente certificatore terzo, il quale, peraltro, dovrà essere designato dalle Autorità nazionali competenti, al fine di garantire la sua indipendenza, la sua competenza, nonché l'assenza di qualsiasi conflitto di interessi[44].

Inoltre, con riferimento ai sistemi IA *safety components* di un prodotto o che costituiscano essi stessi prodotti rientranti nell'ambito di applicazione di determinati atti di diritto derivato, non esiste alcun automatismo, quanto alla considerazione del sistema come ad alto rischio o meno, tra la qualificazione effettuata ai sensi del Regolamento e la corrispondente classificazione in virtù della normativa di settore. In altre parole, per tali *devices* opererà la disciplina prevista dall'atto di diritto derivato di volta in volta applicabile. Così, per esempio, in tema di dispositivi medici di IA (c.d. *software as medical devices* o SaMD), ai sensi del Regolamento UE/2017/745, che prevede, in relazione all'intensità di incidenza potenziale del dispositivo sui parametri clinici dei pazienti, tre macro-classi di rischio (I, II e III) – variamente articolate al loro interno – la valutazione di conformità da parte di un ente certificatore terzo sarà obbligatoria non solo per i *devices* rientranti nella più elevata classe di rischio (III), ma anche per quelli della classe intermedia (II).

4. Considerazioni conclusive: alcune piste di indagine.

In conclusione, si può affermare che la Proposta di Regolamento qui brevemente commentata rappresenta indubbiamente un passo in avanti, da parte delle Istituzioni dell'Unione, verso la regolazione di un fenomeno tecnico-scientifico effettivamente complesso.

Tuttavia, rimangono diverse questioni aperte. Sarà dunque nostro compito, come studiosi, tentare di risolverle, anche alla luce dei vari passaggi dell'*iter* normativo appena inaugurato. *Medio tempore*, sia qui consentita l'individuazione di alcune piste d'indagine.

In primo luogo, salvi i casi in cui la questione sia risolta a monte dal legislatore sovranazionale, al fine di individuare il diritto applicabile, dovranno essere scandagliati i termini di reciproca integrazione tra le disposizioni del futuribile Regolamento (*e.g.* quelle attinenti ai requisiti dei sistemi) e gli atti normativi nazionali e sovranazionali la cui rilevanza verrà, di volta in volta, in considerazione (si pensi, tra le tante tematiche, alla complessa materia dei dispositivi medici).

In secondo luogo, andranno verificate la portata e i limiti di incidenza del Regolamento sul diritto penale italiano, sostanziale e processuale. Per esempio, dovendo gli Stati membri prevedere, al fine di garantire il rispetto degli obblighi regolamentari, delle sanzioni **effettive**, **proporzionate** e **dissuasive** (non essendo previsto, però, alcun obbligo di criminalizzazione – la cui legittimità, del resto, non sarebbe in ogni caso garantita né

[44] Considerando n. 65.

dall'art. 114, né dall'art. 16 TFUE)[45], anzitutto, si dovrà verificare, caso per caso, secondo una valutazione di politica criminale e alla luce del canone di *extrema ratio*, l'effettiva insufficienza di sanzioni amministrative e la conseguente necessità di un presidio di carattere penale; in subordine, in caso di risposta affermativa a tale quesito, bisogneràchiarire se vi siano, nel nostro ordinamento, delle norme incriminatrici *de iure condito* applicabili, valutando se del caso una loro modifica, ovvero l'introduzione di nuovi tipi criminosi.

E, ancora, sotto il profilo processualistico, ci si dovrà interrogare circa i termini di cogenza per il legislatore della disciplina in materia di sistemi di riconoscimento facciale, e più in generale di sistemi con finalità di *law enforcement*. Applicando i criteri elaborati dalla nota giurisprudenza sovranazionale e nazionale (anzitutto costituzionale) in tema di rapporti tra ordinamento UE e ordinamento interno[46], quale destino avrebbe una normativa domestica eventualmente introduttiva, tra i mezzi di ricerca della prova, di sistemi di tal fatta, ma in violazione della disciplina imposta dal Regolamento (la quale prevede, com'è stato segnalato, sia talune salvaguardie, sia l'obbligo in capo ai legislatori di disciplinare dettagliatamente tale materia)?

Per il momento sono più i dubbi che le certezze.

Eppure, in attesa delle riflessioni scientifiche e degli sviluppi normativi sul tema, va salutata con favore l'iniziativa della Commissione, frutto di uno sforzo epocale, finalizzato a evitare che lo sviluppo e l'impiego di sistemi così complessi rimangano oggetto di una *de-regulation* (o meglio *non-regulation*) la quale, anziché garantire un bilanciamento tra le ragioni del progresso tecnico-scientifico ed economico da un lato, e quelle di tutela dei beni giuridici dall'altro, produrrebbe solo un pericoloso squilibrio a danno dei diritti e delle libertà fondamentali.

Bibliografia.

Atti normativi e documenti di carattere politico.

- COM(2018) 237 final.

---

[45] Sul tema delle competenze penali dell'Unione in materia penale v. *amplius* G. Marinucci, E. Dolcini, G.L. Gatta, *Manuale di diritto penale. Parte Generale*, 9ª ed., Giuffrè, 2020, pp. 50 ss.; V. Manes, M. Caianiello, *Introduzione al diritto penale europeo*, Giappichelli, 2020; Aa.Vv., *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona* (a cura di) G. Grasso, L. Picotti, R. Sicurella, Giuffrè, 2011; A. Bernardi, *La competenza penale accessoria dell'Unione europea: problemi e prospettive*, in *Diritto penale contemporaneo – Rivista trimestrale*,Fasc. 1, 2012, pp. 43 ss.

[46] In materia di rapporti tra diritto UE e diritto nazionale, v. ampiamente *ex multis* R. Bin, G. Pitruzzella, *Diritto costituzionale*, 21ª ed., Giappichelli, 2020, pp. 439 ss.; U. Draetta, A. Santini, F. Bestagno, *Elementi di diritto dell'Unione europea. Parte istituzionale: ordinamento e struttura dell'Unione europea*, Giuffrè, 2018, pp. 328 ss.; B. Nascimbene, *La tutela dei diritti fondamentali in Europa: i cataloghi e gli strumenti a disposizione dei giudici nazionali (cataloghi, arsenale dei giudici e limiti o confini)*, in *Eurojus*, Fasc. 3, 2020, 272 ss.; G. Grasso, *Introduzione: Diritto penale e integrazione europea*, in G. Grasso, R. Sicurella (a cura di), *Lezioni di diritto penale europeo*, Giuffrè, 2007, pp. 1 ss.; A. Ruggeri, *L'interpretazione conforme e la ricerca del "sistema di sistemi" come problema*, in A. Bernardi (a cura di), *L'interpretazione conforme al diritto dell'Unione europea. Profili e limiti di un vincolo problematico*, Jovene, 2015, pp. 153 ss.; V. Manes, *Metodo e limiti dell'interpretazione conforme alle fonti sovranazionali in materia penale*, in *ivi*, pp. 391 ss.

- COM(2021) 205 final.
- COM(2021) 206 final.
- Consiglio dell'Unione europea, *Conclusioni sugli spazi di sperimentazione normativa e le clausole di sperimentazione come strumenti per un quadro normativo favorevole all'innovazione, adeguato alle esigenze future e resiliente che sia in grado di affrontare le sfide epocali nell'era digitale*, 13026/20, 16 novembre 2020.
- https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en.

Dottrina.

- Aa.Vv., *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona* (a cura di) G. Grasso, L. Picotti, R. Sicurella, Giuffrè, 2011.
- S. Allegrezza, A. Mosna, *I diritti della difesa*, in S. Allegrezza, R. Mastroianni, O. Pollicino, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, 2017, pp. 946 ss.
- A. Amidei, *La* governance *dell'Intelligenza Artificiale: profili e prospettive di diritto dell'Unione Europea*, in U. Ruffolo, (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, 2020, pp. 571 ss.
- F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *questa rivista*, 10, 2019, 1 ss.
- A. Bernardi, *La competenza penale accessoria dell'Unione europea: problemi e prospettive*, in *Diritto penale contemporaneo – Rivista trimestrale*, Fasc. 1, 2012, pp. 43 ss.
- R. Bin, G. Pitruzzella, *Diritto costituzionale*, 21ª ed., Giappichelli, 2020.
- C. Brusco, *Rischio e pericolo, rischio consentito e principio di precauzione. La c.d. "flessibilizzazione delle categorie del reato"*, in *Criminalia*, 2012, pp. 391 ss.
- M. Caianiello, *Giudice imparziale precostituito e tutela effettiva dei diritti in materia penale*, in S. Allegrezza, R. Mastroianni, O. Pollicino, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, 2017, pp. 903 ss.
- G. Calabresi, *First Party, Third Party, and Product Liability Systems: Can Economic Analysis of Law Tell Us Anything About Them?*, in *Iowa Law Review*, 69, 1984, pp. 833 ss.
- B. Caravita di Torrito, *Principi costituzionali e intelligenza artificiale*, in U. Ruffolo, (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, 2020, pp. 451 ss.
- C. Casonato, *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, in *BioLaw Journal – Rivista di BioDiritto*, Fasc. 2, 2019, pp. 711 ss.
- C. Casonato, *Potenzialità e sfide dell'intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, Fasc. 1, 2019, pp. 177 ss.
- D. Castronuovo, *Principio di precauzione e diritto penale. Paradigmi dell'incertezza nella struttura del reato*, Aracne, 2012.
- R.H. Coase, *The Firm, the Market, and the Law*, University of Chicago Press, 2004.
- E. Corn, *Il principio di precauzione nel diritto penale. Studio sui limiti all'anticipazione della tutela penale*, Giappichelli, 2013.
- M. del Tufo, *Principio di precauzione e gestione del rischio: quali spazi applicativi per il diritto penale?*, in G. Carlizzi, G. Tuzet (a cura di), *La prova scientifica nel processo penale*, Giappichelli, 2018, pp. 137 ss.

- D.P. Domenicucci, F. Filpo, *La tutela giurisdizionale effettiva nel diritto dell'Unione europea*, in S. Allegrezza, R. Mastroianni, O. Pollicino, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, 2017, pp. 864 ss.
- M. Donini, *Un nuovo medioevo penale? Vecchio e nuovo nell'espansione del diritto penale economico*, in *Cass. Pen.*, 6, 2003, pp. 1808 ss.
- U. Draetta, A. Santini, F. Bestagno, *Elementi di diritto dell'Unione europea. Parte istituzionale: ordinamento e struttura dell'Unione europea*,Giuffrè, 2018.
- G. Fiandaca, *Il reato commissivo mediante omissione*, Giuffrè, 1979.
- G. Fiandaca, E. Musco, *Diritto penale. Parte generale*, 8ª ed., Zanichelli, 2019.
- S. Fiore, *La teoria generale del reato alla prova del processo: spunti per una ricostruzione integrata del sistema penale*, ESI, 2007.
- G. Forti, *"Accesso" alle informazioni sul rischio e responsabilità: una lettura del principio di precauzione*, in *Criminalia*, 2006, pp. 155 ss.
- F. Giunta, *Il diritto penale e le suggestioni del principio di precauzione*, in *Criminalia*, 2006, pp. 227 ss.
- G. Grasso, *Il reato omissivo improprio. La struttura obiettiva della fattispecie*, Giuffrè, 1983.
- G. Grasso, *Introduzione: Diritto penale e integrazione europea*, in G. Grasso, R. Sicurella (a cura di), *Lezioni di diritto penale europeo*, Giuffrè, 2007, pp. 1 ss.
- L. Luparia, J. della Torre, *La presunzione di innocenza*, in S. Allegrezza, R. Mastroianni, O. Pollicino, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, 2017, pp. 915 ss.
- V. Manes, M. Caianiello, *Introduzione al diritto penale europeo*, Giappichelli, 2020.
- V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. Ruffolo, (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, 2020, pp. 547 ss.
- V. Manes, *Metodo e limiti dell'interpretazione conforme alle fonti sovranazionali in materia penale*, in A. Bernardi (a cura di), *L'interpretazione conforme al diritto dell'Unione europea. Profili e limiti di un vincolo problematico*, Jovene, 2015, pp. 391 ss.
- G. Marinucci, E. Dolcini, G.L. Gatta, *Manuale di diritto penale. Parte Generale*, 9ª ed., Giuffrè, 2020.
- B. Nascimbene, *La tutela dei diritti fondamentali in Europa: i cataloghi e gli strumenti a disposizione dei giudici nazionali (cataloghi, arsenale dei giudici e limiti o confini)*, in *Eurojus*, Fasc. 3, 2020, 272 ss.
- R. Parenti, *Regulatory Sandboxes and Innovation Hubs for FinTech. Impact on innovation, financial stability and supervisory convergence – Study for the committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament*, 24 settembre 2020.
- F. Pesce, *L'analisi economica del diritto penale dalla teoria alla pratica. Il livello di efficienza delle opzioni normative in tema di tossicodipendenza e criminalità correlata*, Editoriale Scientifica, 2019.
- C. Piergallini, *Danno da prodotto e responsabilità penale. Profili dommatici e politico-criminali*, Giuffrè, 2004.
- R.A. Posner, *Economic Analysis of Law,* 9ª ed., Wolters Kluwer, 2014.
- D.Pulitanò, *Diritto penale*, 8ª ed., Giappichelli, 2019.
- S. Quattroccolo, *Equo processo penale e sfide della società algoritmica*, in *BioLaw Journal – Rivista di BioDiritto*, Fasc. 1, 2019, pp. 135 ss.

- S. Riondato, *Robot: talune implicazioni di diritto penale*, in *Tecnodiritto: temi e problemi di informatica e robotica giuridica* (a cura di) P. Moro, C. Sarra, Milano, Franco Angeli, 2017, pp. 85 ss.
- C.M. Romeo Casabona, *Aportaciones del principio de precaución al derechopenal*, in Id., *Principio de precaución, biotecnología y derecho*, Universidad de Deusto – Universidad de País Vasco – Comares, 2004, pp. 385 ss.
- A. Ruggeri, *L'interpretazione conforme e la ricerca del "sistema di sistemi" come problema*, in A. Bernardi (a cura di), *L'interpretazione conforme al diritto dell'Unione europea. Profili e limiti di un vincolo problematico*, Jovene, 2015, pp. 153 ss.
- S.J. Russell, P. Norvig, *Artificial Intelligence. A Modern Approach*, 4ª ed., Pearson, 2021.
- P. Severino, *Intelligenza artificiale e diritto penale*, in U. Ruffolo, (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, 2020, pp. 531 ss.
- F. Sgubbi, *Responsabilità penale per omesso impedimento dell'evento*, CEDAM, 1975.