Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL
A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

2/2021

Editore Associazione “Progetto giustizia penale”, c/o Università degli Studi di Milano,
Dipartimento di Scienze Giuridiche "C. Beccaria" - Via Festa del Perdono, 7 - 20122 MILANO - c.f. 97792250157
ANNO 2021 - CODICE ISSN 2240-7618 - Registrazione presso il Tribunale di Milano, al n. 554 del 18 novembre 2011.
Impaginazione a cura di Chiara Pavesi

Diritto penale contemporaneo – Rivista trimestrale è un periodico on line ad accesso libero e non ha fine di profitto. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione. La rivista, registrata presso il Tribunale di Milano, al n. 554 del 18 novembre 2011, è edita attualmente dall'associazione "Progetto giustizia penale", con sede a Milano, ed è pubblicata con la collaborazione scientifica e il supporto dell'Università Commerciale Luigi Bocconi di Milano, dell'Università degli Studi di Milano, dell'Università di Roma Tre, dell'Università LUISS Guido Carli, dell'Universitat de Barcelona e dell'Università Diego Portales di Santiago del Cile.

La rivista pubblica contributi inediti relativi a temi di interesse per le scienze penalistiche a livello internazionale, in lingua italiana, spagnolo, inglese, francese, tedesca e portoghese. Ogni contributo è corredato da un breve abstract in italiano, spagnolo e inglese.

La rivista è classificata dall'ANVUR come rivista scientifica per l'area 12 (scienze giuridiche), di classe A per i settori scientifici G1 (diritto penale) e G2 (diritto processuale penale). È indicizzata in DoGI e DOAJ.

La rivista può essere citata in forma abbreviata con l'acronimo: *DPC-RT*, corredato dall'indicazione dell'anno di edizione e del fascicolo.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Committee on Publication Ethics).

La rivista si conforma alle norme del Regolamento UE 2016/679 in materia di tutela dei dati personali e di uso dei cookies (clicca qui per dettagli).

Ogni contributo proposto per la pubblicazione è preliminarmente esaminato dalla direzione, che verifica l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

In caso di esito positivo di questa prima valutazione, la direzione invia il contributo in forma anonima a due revisori, individuati secondo criteri di rotazione tra i membri dell'Editorial Advisory Board in relazione alla rispettiva competenza per materia e alle conoscenze linguistiche. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore.

La direzione comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se entrambe le valutazioni sono positive, il contributo è pubblicato. Se una o entrambe le valutazioni raccomandano modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se uno o entrambi i revisori esprimono parere negativo alla pubblicazione.

La direzione si riserva la facoltà di pubblicare, in casi eccezionali, contributi non previamente sottoposti alla procedura di peer review. Di ciò è data notizia nella prima pagina del contributo, con indicazione delle ragioni relative.

I contributi da sottoporre alla Rivista possono essere inviati al seguente indirizzo mail: editor.criminaljusticenetwork@gmail.com. I contributi che saranno ritenuti dalla direzione di potenziale interesse per la rivista saranno sottoposti alla procedura di peer review sopra descritta. I contributi proposti alla rivista per la pubblicazione dovranno rispettare i criteri redazionali scaricabili qui.

Diritto penale contemporaneo – Rivista trimestrale es una publicación periódica *on line*, de libre acceso y sin ánimo de lucro. Todas las colaboraciones de carácter organizativo y editorial se realizan gratuitamente y no se imponen a los autores costes de maquetación y publicación.
La Revista, registrada en el Tribunal de Milan, en el n. 554 del 18 de noviembre de 2011, se edita actualmente por la asociación "Progetto giustizia penale", con sede en Milán, y se publica con la colaboración científica y el soporte de la *Università Commerciale Luigi Bocconi* di Milano, la *Università degli Studi di Milano,* la *Università di Roma Tre*, la *Università LUISS Guido Carli*, la *Universitat de Barcelona* y la *Universidad Diego Portales de Santiago de Chile.*
La Revista publica contribuciones inéditas, sobre temas de interés para la ciencia penal a nivel internacional, escritas en lengua italiana, española, inglesa, francesa, alemana o portuguesa. Todas las contribuciones van acompañadas de un breve abstract en italiano, español e inglés.
El lector puede leer, compartir, reproducir, distribuir, imprimir, comunicar a terceros, exponer en público, buscar y señalar mediante enlaces de hipervínculo todos los trabajos publicados en "Diritto penale contemporaneo – Rivista trimestrale", con cualquier medio y formato, para cualquier fin lícito y no comercial, dentro de los límites que permite la licencia *Creative Commons - Attribuzione - Non commerciale 3.0 Italia* (CC BY-NC 3.0 IT) y, en particular, debiendo mantenerse la indicación de la fuente, el logo, el formato gráfico original, así como el autor de la contribución.
La Revista se puede citar de forma abreviada cn el acrónimo *DPC-RT*, indicando el año de edición y el fascículo.
La Revista asume el Code of Conduct and Best Practice Guidelines for Journal Editors elaborado por el COPE (*Comitte on Publication Ethics*).
La Revista cumple lo dispuesto en el Reglamento UE 2016/679 en materia de protección de datos personales (clica aquí para los detalles sobre protectión de la privacy y uso de cookies).
Todas las contribuciones cuya publicación se propone serán examinadas previamente por la Dirección, que verificará la correspondencia con los temas tratados en la Revista y el respeto de los requisitos mínimos para su publicación.
En el caso de que se supere con éxito aquella primera valoración, la Dirección enviará la contribución de forma anónima a dos evaluadores, escogidos entre los miembros del *Editorial Advisory Board*, siguiendo criterios de rotación, de competencia por razón de la materia y atendiendo también al idioma del texto. Los evaluadores recibirán un formulario, que deberán devolver a la Dirección en el plazo indicado. En el caso de que la devolución del formulario se retrasara o no llegara a producirse, la Dirección se reserva la facultad de escoger un nuevo evaluador.
La Dirección comunicará el resultado de la evaluación al autor, garantizando el anonimato de los evaluadores. Si ambas evaluaciones son positivas, la contribución se publicará. Si alguna de las evaluaciones recomienda modificaciones, la contribución se publicará después de que su autor la haya revisado sobre la base de los comentarios recibidos y de que la Dirección haya verificado que tales comentarios han sido atendidos. La contribución no se publicará cuando uno o ambos evaluadores se pronuncien negativamente sobre su publicación.
La Dirección se reserva la facultad de publicar, en casos excepcionales, contribuciones que no hayan sido previamente sometidas a *peer review*. Se informará de ello en la primera página de la contribución, indicando las razones.

Si deseas proponer una publicación en nuestra revista, envía un mail a la dirección editor.criminaljusticenetwork@gmail.com. Las contribuciones que la Dirección considere de potencial interés para la Revista se someterán al proceso de *peer review* descrito arriba. Las contribuciones que se propongan a la Revista para su publicación deberán respetar los criterios de redacción (se pueden descargar aquí).

Diritto penale contemporaneo – Rivista trimestrale is an on-line, open-access, non-profit legal journal. All of the organisational and publishing partnerships are provided free of charge with no author processing fees. The journal, registered with the Court of Milan (n° 554 - 18/11/2011), is currently produced by the association "Progetto giustizia penale", based in Milan and is published with the support of Bocconi University of Milan, the University of Milan, Roma Tre University, the University LUISS Guido Carli, the University of Barcelona and Diego Portales University of Santiago, Chile.

The journal welcomes unpublished papers on topics of interest to the international community of criminal scholars and practitioners in the following languages; Italian, Spanish, English, French, German and Portuguese. Each paper is accompanied by a short abstract in Italian, Spanish and English.

For citation purposes the journal's abbreviated reference format may be used: *DPC-RT,* indicating year of publication and issue.

The journal strictly adheres to the Code of Conduct and Best Practice Guidelines for Journal Editors drawn up by COPE (Committee on Publication Ethics).

The journal complies with the General Data Protection Regulation (EU) 2016/679 (GDPR) (click here for details on protection of privacy and use of cookies).

All articles submitted for publication are first assessed by the Editorial Board to verify pertinence to topics addressed by the journal and to ensure that the publication's minimum standards and format requirements are met.

Should the paper in question be deemed suitable, the Editorial Board, maintaining the anonymity of the author, will send the submission to two reviewers selected in rotation from the Editorial Advisory Board, based on their areas of expertise and linguistic competence. The reviewers are provided with a feedback form to compile and submit back to the editorial board within an established timeframe. If the timeline is not heeded to or if no feedback is submitted, the editorial board reserves the right to choose a new reviewer.

The Editorial Board, whilst guaranteeing the anonymity of the reviewers, will inform the author of the decision on publication. If both evaluations are positive, the paper is published. If one or both of the evaluations recommends changes the paper will be published subsequent to revision by the author based on the comments received and verification by the editorial board. The paper will not be published should one or both of the reviewers provide negative feedback.

In exceptional cases the Editorial Board reserves the right to publish papers that have not undergone the peer review process. This will be noted on the first page of the paper and an explanation provided.

If you wish to submit a paper to our publication please email us at editor.criminaljusticenetwork@gmail.com. All papers considered of interest by the editorial board will be subject to peer review process detailed above. All papers submitted for publication must abide by the editorial guidelines (download here).

Contents

Contents

Contents

Giustizia penale e nuove tecnologie
Justicia penal y nuevas tecnologías
Criminal Justice and New Technologies

La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale

La nueva propuesta europea para regular los sistemas de inteligencia artificial en el ámbito de la justicia penal

The New Draft for an EU AI Regulation and Its Relevance for Criminal Justice

Anita Lavorgna e Gabriele Suffia

Professoressa Associata di Criminologia, Università di Southampton (Regno Unito) a.lavorgna@soton.ac.uk

Assegnista di ricerca, Università degli Studi di Milano (Italia) gabriele.suffia@unimi.it

Intelligenza artificiale | Inteligencia artificial | Artificial Intelligence

Abstracts

La Commissione Europea ha recentemente pubblicato una proposta di Regolamento che mira a gestire e controllare i rischi dovuti all'uso dei Sistemi di Intelligenza Artificiale (SIA). Siccome questi sistemi vengono sempre più utilizzati sia nell'ambito della prevenzione e del contrasto al crimine che nell'amministrazione della giustizia, la proposta di regolamento è di grande rilievo nell'ambito della giustizia penale. Questo contributo si propone di fornire un'analisi della bozza pubblicata alla luce delle discussioni accademiche in materia che sono avvenute negli ultimi anni, cercando di capire se, e fino a che punto, la proposta della Commissione risponde adeguatamente alle criticità sollevate o appurate con riferimento ad alcuni usi dei cosiddetti SIA, con una specifica attenzione a quelli con effetti diretti nell'ambito della giustizia penale.

La Comisión Europea ha recientemente publicado una propuesta de reglamento que pretende gestionar y controlar los riesgos derivados del uso de sistemas de inteligencia artificial (SIA). Dado que estos sistemas se utilizan cada vez más, tanto en el ámbito de la prevención del delito y la aplicación de la ley como en el de la administración de justicia, el proyecto de reglamento es de gran relevancia en el ámbito de la justicia penal. Este trabajo tiene por objeto ofrecer un análisis del proyecto publicado a la luz de las discusiones académicas relevantes que han lugar en los últimos años, tratando de comprender si, y en qué medida, la propuesta de la Comisión responde adecuadamente a las cuestiones críticas constatadas en referencia a algunos usos de los denominados SIA, centrándose específicamente en los que tienen efectos directos en el contexto de la justicia penal.

The European Commission has recently published a draft AI Regulation aiming at managing and curbing some of the risks linked to using Artificial Intelligence Systems (AISs). As these systems are increasingly used both in the context of crime prevention and control, and in the administration of justice, the draft Regulation is of great relevance from a criminal justice perspective. This paper offers an analysis of the published draft stemming from the recent academic debate on the topic and discusses whether and to what extent the current draft takes into sufficient account the main criticisms raised against the use of AISs, especially in the criminal justice arena.

Sommario

1. Introduzione.

Nel dibattito specialistico, particolarmente nell'ultimo quinquennio, vi è stato un riconoscimento crescente dei rischi legati all'uso delle Intelligenze Artificiali (IA) – definite in modo ampio come quelle tecnologie alla base di sistemi in grado di analizzare il proprio ambiente e compiere azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi[1]. Queste, infatti, sono tecnologie che spesso hanno un effetto, o un potenziale, trasformativo[2], ma che al momento sono sottoposte a pochissimi limiti e controlli. Ciononostante, le IA sono già ampiamente usate, non solo per rendere più efficienti certi servizi al pubblico o alcuni processi produttivi[3], ma anche in settori "sensibili" come quello della giustizia penale[4], venendo applicate in molti sistemi giudiziari e di polizia per "prevedere" – tra le altre cose – fattori di rischio[5], *hotspot* criminali[6], o per implementare l'identificazione biometrica di determinati individui[7].

Il vuoto legislativo attuale sembra però destinato ad esaurirsi, e con esso il lungo periodo di auto-regolamentazione che ha caratterizzato la materia, in constante espansione, dagli anni '70 in poi[8]. La Commissione Europea ha infatti recentemente pubblicato una proposta di Regolamento sul tema, focalizzata sul gestire e controllare i rischi dovuti all'uso dell'IA o, per essere più precisi, come vedremo, dei Sistemi di Intelligenza Artificiale (da qui in poi, SIA)[9]. La pubblicazione di questa bozza non sorprende: l'avvento di nuova legislazione in materia è stato all'orizzonte da tempo. Del resto la Commissione, come discusso in una specifica Comunicazione[10], ha espressamente riconosciuto come, di fronte agli sviluppi delle IA e al loro crescente utilizzo a livello globale, si renda necessario un intervento legislativo di co-regolamentazione[11] con una visione, capace di guardare al futuro, volta a rendere l'Unione Europea un centro di rilevanza mondiale nel settore (una precondizione, secondo la Comunicazione, per la prosperità e competitività dell'Unione), garantendo al contempo un uso etico delle nuove tecnologie, mantenendo l'essere umano al centro[12].

Questo contributo si propone di fornire un'analisi della bozza pubblicata alla luce delle discussioni accademiche in materia che sono avvenute negli ultimi anni, cercando di capire se, e fino a che punto, la proposta della Commissione risponde adeguatamente alle criticità sollevate o appurate con riferimento ad alcuni usi dei cosiddetti SIA, con una specifica attenzione a quelli con effetti diretti nell'ambito della giustizia penale.

2. L'Intelligenza Artificiale, i suoi rischi, e l'algoretica come necessità.

Negli ultimi anni sono emersi una moltitudine di approcci in ambito di IA, utilizzati negli ambiti più vari – si pensi, a titolo esemplificativo, alle assicurazioni, alla didattica, e persino ai giocattoli per l'infanzia[13]. Nella letteratura penalistica e criminologica, gli ambiti più studiati

[1] Definizione adattata da COMMISSIONE EUROPEA 82018). Si veda anche Finocchiaro (2019).
[2] Si veda ad esempio Gruetzemacher e Whittlestone (2019).
[3] Si pensi, ad esempio, a Cioffi *et al.* (2020), p.492; Meyer *et al.* (2020).
[4] Per una recente metanalisi si veda Lavorgna e Uwgudike (2021).
[5] Si veda ad esempio Angwin e Larson (2016); Oswald *et al.* (2018).
[6] Lum e Isaac (2016); Ensign *et al.* (2018).
[7] Bennet Moses e Chan (2018); Fussey e Murray (2019).
[8] Esposito (2013).
[9] COMMISSIONE EUROPEA (2021a).
[10] Si veda COMMISSIONE EUROPEA (2021b).
[11] In quanto interviene nell'ottica del *risk assessment*, concentrando i propri sforzi nella responsabilizzazione degli attori coinvolti nei SIA.
[12] COMMISSIONE EUROPEA (2021b), pp.1 e 9.
[13] Si consideri ad esempio: Cevolini e Esposito (2020); Prinsloo (2020); Mcstay e Rosner (2021).

sono quelli in cui SIA sono stati ideati, o utilizzati, ai fini di prevenzione della criminalità, per facilitare azioni di polizia e analisi investigative, e in ambito giudiziario. Strumenti come il *social media mining* (l'estrazione di enormi quantità di dati grezzi sui social media per identificare tendenze comportamentali), *sentiment analysis* (il processo di identificazione computazionale del "tono emotivo" dietro un pezzo di testo), *natural language processing* (l'applicazione di tecniche computazionali per analizzare le interazioni tra computer e linguaggi umani), tecnologie di *machine learning* (SIA che consentono ai sistemi informatici di apprendere e migliorare le prestazioni in un determinato compito senza essere esplicitamente programmati per farlo) e numerose applicazioni software biometriche (utili, ad esempio, per verificare l'identità di una persona analizzandone identificatori di tipo fisico) sono solo alcuni degli strumenti che vengono sempre più proposti e, in alcuni casi, utilizzati anche per la prevenzione della criminalità, o per rendere più efficaci ed efficienti – almeno secondo chi li promuove – i nostri sistemi di giustizia penale[14].

In questo contesto, il rapido aumento delle SIA evidenzia la loro crescente popolarità come strumenti di prevenzione e controllo della criminalità, nonostante una mole crescente di studi indichi i danni sociali (*social harms*) ad essi associati[15]. Esiste infatti un *corpus* di letteratura critica, in rapida crescita, sulla proliferazione della "datificazione" e sull'uso di SIA nell'ambito della giustizia penale. È stato evidenziato come le potenzialità di questi approcci basati sull'IA, seppure incoraggianti in un'ottica di aumento dell'efficienza del sistema, siano eccessivamente enfatizzate da utopici "immaginari sociotecnici"[16] che sottolineano i benefici della algoritmizzazione e della datificazione alla loro base offuscandone però i limiti e i danni sociali (e specialmente i cosiddetti *technological harms*)[17]. Questi immaginari sono spesso promossi da coloro che più detengono e maneggiano il cosiddetto "capitale digitale"[18], ovvero le risorse necessarie non solo per lo sviluppo tecnologico, ma anche per definire le narrative dominanti che circondano il suo utilizzo (col settore privato e ricercatori in discipline computazionali in prima linea)[19].

Come anticipato, l'impiego dei SIA e dei dati utilizzati per il loro "addestramento" in ambito di prevenzione e controllo della criminalità non è privo di problemi. In primo luogo, vi sono sfide tecniche da affrontare, che si possono riassumere in un problema di falsi positivi/falsi negativi. A titolo esemplificativo, si ricorda come i *big data*, soprattutto quando vanno analizzati in tempo reale o quando vengono utilizzati per identificare situazioni e incidenti che richiedono una risposta immediata, non sono facili da gestire, in quanto dati importanti possono andare persi nel "rumore di fondo" generato da dati inutili e potenzialmente fuorvianti. In secondo luogo, soprattutto per quanto riguarda la polizia predittiva – ovvero l'uso di tecniche analitiche di tipo statistico per prevenire certe forme di criminalità, ad esempio individuando obiettivi probabili sui quali focalizzare i controlli – non vi sono certezze fattuali fornite dai dati, ma solo proiezioni statistiche basate su modelli computazionali. Spesso questi dati sono imperfetti, in quanto insufficienti nel fornire una rappresentazione accurata della complessità della realtà sociale, o creati e raccolti per scopi diversi e solo in un secondo momento utilizzati per raggiungere uno scopo in carenza di dati migliori (si pensi, banalmente, a come abitare in un determinato quartiere possa essere utilizzato per inferire il reddito, o la propensione alla criminalità; o all'analisi automatica dei *tweet* per avere notizie in tempo reale su un evento pubblico, in cui il contesto ad esempio ironico di un post potrebbe non essere colto da un software). Anche in presenza di dati raccolti e processati con cura, a causa della complessità del comportamento umano, i modelli ottenuti sono generalmente spuri e vulnerabili al cambiamento[20].

Inoltre, è ormai ampiamente riconosciuto come le minoranze – ad esempio quelle etniche – siano più vulnerabili all'applicazione erronea dei SIA, a causa della loro sottorappresentazio-

[14] Si veda ad esempio: Hardns e Rummens (2017); Williams *et al.* (2017); Aghababei e Makrechi (2018); Završnik (ed.) (2018); Cohen (2019).
[15] Barocas e Selbest, (2016); Ferguson (2017); Oswald *et al.* (2018); Hao e Stray (2019); Lavorgna e Uwgudike (2021).
[16] Prendendo in prestito le parole di JASANOFF (2015).
[17] "Danni sociali" ormai riconosciuti da varie discipline, come emerge da studi criminologici (e.g., Hannah-Moffat (2018); Ugwudike (2020)), giuridici (e.g. , Custers (2013); Starr (2014); Hamilton (2015)), di sociologia dei processi comunicativi (e.g., Iliadis e Russo (2016)) e di informatica (e.g., Hao e Stray (2019)).
[18] Van Dijk (2005).
[19] Cfr. Lavorgna e Uwgudike (2021).
[20] Smith *et al.* (2017).

ne/iper-rappresentazione nei dati sui quali molti SIA si basano[21]. Conseguentemente, alcuni SIA possono rafforzare pregiudizi preesistenti nelle nostre società e nelle attività di polizia e giudiziarie, rischiando di rafforzare processi sociali di "etichettatura" (*labelling*) in senso negativo[22], di perpetuare l'ipercontrollo verso di alcuni segmenti della popolazione, e financo di trascurare principi fondamentali come la presunzione di innocenza[23]. Del resto, i modelli sono validi solo quanto i dati su cui sono costruiti e "addestrati", e questi dati – ormai lo sappiamo bene – hanno spesso problemi legati, ad esempio, a pregiudizi razziali o di genere.

Non va infine dimenticato come, in un ambito di giustizia penale, i SIA si rivolgano ovviamente ad un utilizzo pubblico, per finalità di polizia o di giustizia; allo stesso modo, l'origine di molti dati è pubblica, o affidata agli utenti stessi. Lo sviluppo di SIA, invece, è generalmente compito di sviluppatori e altri "tecnici" che, ad oggi, sono per lo più privati di grandi dimensioni e multinazionali (seppur spesso finanziati con commesse pubbliche). Ne consegue uno scenario in cui l'Autorità pubblica, specie singola, è impossibilitata a intervenire sul software che utilizza al fine di correggerlo o adattarlo a nuove sopraggiunte esigenze, senza dover fare affidamento all'intervento del produttore. Non sembra una prospettiva di poco conto, nel momento in cui la forza di un SIA risiede proprio nella possibilità di addestrarlo e modificarlo secondo le proprie esigenze di utilizzo. Come conseguenza, di fatto, si ha che aziende private hanno sempre più potere di incidere su diritti fondamentali, che potrebbero essere minacciati da algoritmi "irresponsabili".

Alla luce di quanto discusso, non dovrebbe dunque sorprendere come la letteratura criminologica e sociologica abbiano a lungo sottolineato l'importanza di comprendere le teorie e i limiti alla base dei modelli di IA utilizzati per essere in grado di valutare criticamente i risultati da loro proposti, e di utilizzare i *big data* in ambito di giustizia penale solo in combinazione con forme di dati più affidabili[24]. Sfortunatamente, uno dei problemi di fondo da affrontare al momento è che molti utenti che si affidano ai SIA, siano essi decisori politici, forze di polizia, aziende o privati cittadini, spesso non hanno quel capitale digitale discusso prima (*i.e.*, le risorse necessarie sia per lo sviluppo tecnologico che per definire le narrative dominanti che circondano il suo utilizzo), e potrebbero sopravvalutare l'affidabilità di questi risultati, in quanto potrebbero non comprendere appieno i meccanismi alla loro base – con conseguenze nefaste dal punto di vista sia pratico che etico, minacciando libertà civili e aumentando disuguaglianze sociali.

L'introduzione di sistemi di revisione formale dei SIA[25], e la predilezione per SIA di tipo socio-tecnico (ovvero che prevedono la presenza di un essere umano in momenti chiave, anziché la totale automatizzazione di certi processi)[26], sono alcuni degli strumenti proposti per mitigare queste problematiche, in linea con la letteratura che sempre più guarda a questioni di etica in ambito di SIA[27], o che si occupa di "IA Responsabile"[28]. In altre parole, al rischio di "algocrazia" (il "dominio degli algoritmi", ovvero la condizione in cui ci troviamo ora e in prospettiva ci troveremmo sempre più, con il massiccio utilizzo di algoritmi per l'organizzazione e il controllo della società) si contrappone dunque l'"algoretica"[29]: si rende necessario uno studio dei problemi etici e dei risvolti sociali (ma anche politici, economici e organizzativi) che derivano dall'uso sempre maggiore delle tecnologie informatiche, *in primis* i SIA. Per "etica" si intende la valorizzazione del tema della scelta in tutto il ciclo della elaborazione delle tecnologie: dalle linee di ricerca fino alla progettazione, la produzione, la distribuzione e l'utente finale.

[21] Per approfondire, si veda ad esempio Harcourt (2015); Eaglin (2017); Ferguson (2017); Hannah-Moffat (2018); LAW SOCIETY (2019); Ugwudike (2020).
[22] Becker (1963).
[23] Ferguson (2012); Shapiro (2017). E' questo un problema riconosciuto, ma solo parzialmente affrontato, anche nel contesto del Regolamento Generale sulla Protezione dei Dati (RGPD). Si veda sul punto Wachter *et al.* (2017); Brkan (2019).
[24] Ad esempio, Chan e Bennet Moses (2015); Williams *et al.* (2017); Lavorgna (2020).
[25] Come proposto in Lavorgna *et al.* (2020).
[26] Si veda ad esempio Ubertis (2020); Middleton (2021).
[27] Si veda, tra le molteplici pubblicazioni recenti in materia, Dubber *et al.* (2020); Kearns e Roth (2020).
[28] Si veda, ad esempio, il rapporto pubblicato dall'INTERNATIONAL TECHNOLOGY LAW ASSOCIATION (2019/2021)e il NIST (2020/2021) *draft whitepaper*. Simili indicazioni derivano anche dal documento del MISE (2020).
[29] Secondo l'idea di Paolo Benanti, frate francescano del Terzo Ordine Regolare e docente di Teologia morale e Bioetica alla Pontificia Università Gregoriana. Cfr. Benati (2018 e 2020). Si veda anche Lombardi-Vallauri (2017), Celotto (2019), e Villalba (2020), p.62.

3. La proposta di Regolamento Europeo.

Tramite 108 pagine di bozza di Regolamento e 17 di allegati, la Commissione si propone esplicitamente di creare una leadership globale per l'Unione Europea nel settore delle IA[30], e da questa prospettiva la proposta recentemente pubblicata dovrebbe concederle il "vantaggio del tratto". Qualora fosse approvato, il Regolamento ora in bozza sarebbe applicabile ad un'ampia casistica sull'uso di SIA, offrendo regole comuni per mettere ordine tra una serie di principi cardine, regole che ambiscono ad essere proporzionate e flessibili: del resto, la necessità è quella di bilanciare il bisogno di mitigare i rischi, ed in particolare quelli inerenti l'uso inappropriato dell'IA, con la necessità di supportare l'innovazione e gli utilizzi opportuni ed appropriati di questi approcci tecnologici (recenti, nuovi o in evoluzione) ormai imprescindibili. Si noti ancora una volta come nella proposta non venga regolata l'IA in quanto tale, ma si regola piuttosto l'ingresso nel mercato, la messa in uso e l'utilizzo nell'ambito dell'Unione dei sistemi che contengono tale tecnologia (*AI Systems* o Sistemi di Intelligenza Artificiale, qua SIA), nel tentativo di mantenere quanta più neutralità nei confronti della tecnologia in discussione, e per non rischiare una veloce obsolescenza definitoria.

La proposta, immediatamente accusata di essere "ampia e vaga" anche se certamente "ambiziosa"[31], è organizzata in 12 Titoli. In questo contributo ci focalizziamo sui primi quattro Titoli, che definiscono lo scopo della proposta e le questioni definitorie (Titolo I), e identificano diverse categorie di IA ai fini di regolamentazione, distinte secondo un approccio basato sul loro diverso rischio: (1) SIA proibiti (Titolo II); (2) SIA ad alto rischio (Titolo III); (3) SIA che richiedono una specifica regolamentazione in quanto pongono specifici rischi di manipolazione (Titoli IV). Dal punto di vista logico, si individua infine in (4) una categoria residuale (altri tipi di SIA).

Innanzitutto, i SIA vengono definiti (art.3(1)) come software sviluppato con una o più tra le tecniche e approcci elencati nell'Allegato I e che, data una serie di obiettivi definiti da un essere umano, possono creare risultati come contenuti, predizioni, raccomandazioni, o decisioni al fine di influenzare l'ambiente col quale interagiscono[32]. Il rimando al primo allegato è chiaramente utile per facilitare le modifiche che si renderanno necessarie alla luce delle innovazioni tecnologiche che sicuramente avverranno nell'ambito delle IA negli anni a venire.

Le sottosezioni a seguire riassumono i punti più salienti delle categorie di SIA ai fini di considerazioni di giustizia penale.

3.1. *SIA proibiti.*

Una serie di SIA vengono proibiti in quanto i rischi a loro legati, o potenzialmente legati, vengono ritenuti inaccettabili. Questi SIA comprendono pratiche che hanno un potenziale significativo di manipolare le persone attraverso tecniche subliminali che vanno oltre la loro coscienza, o di sfruttare le vulnerabilità di specifici gruppi come bambini o persone con disabilità, al fine di distorcere materialmente i loro comportamenti in una maniera che potrebbe verosimilmente causare a loro o a un'altra persona danni fisici o psicologici. Tra i SIA proibiti vengono considerate anche pratiche da parte o per conto dell'autorità pubblica ai fini di valutazione o classificazione dell'affidabilità delle persone fisiche per un certo periodo di tempo, sulla base del comportamento sociale o personale, o della loro personalità nota o prevista, in quanto questo possa portare a un "punteggio sociale" con conseguenze dannose o sfavorevoli per l'interessato (si veda art. 5(1)).

Di maggiore rilevanza nell'ambito della giustizia penale, sono vietati anche i sistemi "a tempo reale" di identificazione biometrica da remoto in spazi pubblici per funzioni di polizia,

[30] COMMISSIONE EUROPEA (2021b), p.7. Questa volontà della Commissione sembra allinearsi al ruolo che essa ha avuto nel definire internazionalmente standard in materia di trattamento dei dati personali e di privacy col Regolamento Generale sulla Protezione dei Dati (RGPD o GDPR in inglese).

[31] Cfr. L'intervento di Peeters *et al.* (2021).

[32] Tra le tecniche e gli approcci di IA, l'Allegato I elenca: approcci di *machine learning* (supervisionati, non supervisionati o di rinforzo, e basati su una varietà di metodi incluso il *deep learning* – ovvero si considerano anche quegli approcci in cui è l'algoritmo a trovare un criterio di classificazione dei dati, trovando le classi, o etichette, da assegnare agli esempi, e la loro gerarchia); approcci basati su logica e conoscenza, inclusa la programmazione induttiva e il ragionamento simbolico; e approcci statistici, inclusi quelli relativi a metodi di stima, ricerca e ottimizzazione.

se a fini si sorveglianza indiscriminata. Sono questi sistemi che certamente possono essere di supporto alla capacità operativa delle forze dell'ordine in contesti caotici e di grandi folle, ma che possono aprire la strada a discriminazioni ed abusi se usati in maniera sommaria o generica, come discusso precedentemente. La bozza prevede tuttavia varie eccezioni che paiono ammettere il loro uso (art. 5(2-4)), e che paiono basarsi su parametri di valutazione "caso per caso" che prendono in considerazione la natura della situazione, le conseguenze dell'uso del SIA, e criteri di proporzionalità.

Nei SIA considerati a rischio inaccettabile rientrano alcune casistiche del riconoscimento facciale, specialmente laddove sia un'autorità pubblica ad utilizzarlo. Le disposizioni proposte nel Regolamento ricalcano alcune note e prese di posizione che già da alcuni mesi l'Unione Europea sta adottando in materia, ma non sono ugualmente esenti da critiche da parte delle associazioni più attente alla privacy[33]. Queste, già nei mesi scorsi avevano chiesto una completa moratoria dei sistemi di riconoscimento facciale all'interno dei paesi dell'Unione, dal momento che i) troppo spesso vi sono stati degli errori importanti, che non sembrano eliminabili neanche in futuro; ii) l'invasione nella sfera privata degli individui è particolarmente significativa. La bozza ammette invece sistemi di riconoscimento facciale in presenza di una serie di importanti eccezioni, ad esempio (artt. 5(1d)): i) per trovare potenziali vittime di un reato (ammesso che la ricerca sia diretta verso uno specifico obiettivo e su specifiche potenziali vittime, per esempio nel caso di bambini scomparsi); ii) per affrontare alcune "minacce sostanziali e imminenti" all'incolumità personale (per esempio, un potenziale attacco terroristico); iii) per il riconoscimento, la localizzazione, l'identificazione o la conduzione di indagini contro sospetti per reati che comportino una pena detentiva (per un minimo di tre anni).

3.2. *SIA ad alto rischio.*

Nell'ambito della bozza di Regolamento, la classificazione di un SIA come "ad alto rischio" dipende dallo scopo per cui tale SIA è previsto, dalla severità dei danni potenziali, e dalla probabilità della loro occorrenza[34]. È questa una norma da considerarsi in concomitanza con la legislazione in materia di sicurezza dei prodotti. I SIA ad alto rischio non sono proibiti in quanto tali, ma sono soggetti a requisiti aggiuntivi (specificati nei Capitoli 2-6); tra le altre cose, questi SIA pongono una serie di obblighi ulteriori ai fornitori di tali sistemi, inclusi obblighi in materia di gestione di dati e metadati, trasparenza, consenso informato, controlli non automatizzati, sicurezza dei sistemi. È anche prevista la creazione di una sorta di registro europeo delle SIA ad alto rischio (art. 60).

I SIA che ricadono in questa categoria sono elencati nell'Allegato III, e riassumendo sono quelli usati per l'identificazione biometrica e la categorizzazione di individui (escludendo i SIA inquadrati come "proibiti"); la gestione e l'operatività di infrastrutture critiche; quelli utilizzati per scopi educativi e di formazione; quelli utilizzati a fine di assunzione e gestione della forza lavoro, o per l'accesso e il godimento di servizi essenziali di natura pubblica o privata; quelli utilizzati dalle forze di polizia, o nella gestione di questioni in materia di immigrazione e asilo; quelli utilizzati nell'amministrazione della giustizia e dei processi democratici. Nell'ambito della giustizia penale, quella dei SIA ad alto rischio può essere considerata la categoria prevalente, più comune.

3.3. *SIA con specifici rischi di manipolazione e altri tipi di SIA.*

Nei SIA che potrebbero essere soggetti a manipolazione il rischio viene valutato come di tipo medio. Si pensi, ad esempio, ai *chatbot* o ad altri sistemi di risposta automatica per fornire assistenza online. Per questi SIA è comunque prevista una serie di controlli, principalmente al fine di evitare o minimizzare eventuali problemi di trasparenza (art. 52). Questi possono

[33] Fortemente critico con il riconoscimento facciale si è dimostrato l'EDPS (European Data Protection Supervisor), così come Amnesty International o le associazioni che fanno riferimento alla campagna "Reclaim Your Face" (https://reclaimyourface.eu/the-movement/) tra cui l' Hermes Center for Transparency and Digital Human Rights in Italia, e alla campagna "Ban Facial Recognition" (https://www.banfacialrecognition.com). Una posizione più articolara ha assunto, invece, l'EFF – Electonic Frontier Foundation.
[34] COMMISSIONE EUROPEA (2021b), p.6.

riguardare sia i dati (vi è dunque la necessità di assicurarsi che i dati non contengano, ad esempio, errori o pregiudizi) che i sistemi stessi (è questo il rifiuto delle cosiddette *black box*, ovvero sistemi in cui non si conosce cosa avviene all'interno del sistema stesso). Per questi SIA, ad esempio, viene richiesto che il funzionamento venga descritto in modo preciso e comprensibile sia per le autorità competenti che per agli utenti. Un video di *deepfake* (*i.e.*, una tecnica basata sull'IA per combinare e sovrapporre immagini e video, usata per creare video falsi), ad esempio, verrebbe obbligatoriamente etichettato come *artificially generated or manipulated* (art. 52(3)), con ciò permettendo all'utente di interrompere la visione; un *chatbot* dovrebbe sottostare allo stesso regime di trasparenza, in modo da permettere all'utente di interrompere lo "scambio" e provare, se possibile, a richiedere l'intervento di una controparte umana.

Infine, non va dimenticata l'esistenza di una categoria residuale, ovvero quei SIA per i quali il rischio è considerato minimo (si pensi a filtri contro lo spam), e per i quali dunque vi sono meri obblighi di indicazione dell'utilizzo nella fornitura di un servizio.

Queste categorie di SIA non vengono esplicitamente discusse con riferimento al sistema penale nella bozza di Regolamento, ma si può certamente ipotizzare una loro applicazione in sistemi, ad esempio, di gestione del sistema o nei rapporti col pubblico.

Profili di criticità.

Per quanto la bozza sia certamente meritevole nel prendere atto di alcuni problemi fondamentali legati a certi SIA, riconoscendo alcuni dei rischi legati all'utilizzo di questi sistemi nell'ambito della giustizia penale, riteniamo che la bozza al momento soffra di una serie di profili di criticità, di seguito riportati.

4.1. *Criticità di scopo.*

Una prima criticità da sollevare riguardo alla proposta di regolamento è quella della definizione di IA[35]. In letteratura non esiste, infatti, una definizione unanimemente condivisa, motivo per il quale si è deciso di adottare un approccio a elencazione, e di focalizzarsi sui SIA. Questa scelta, tuttavia, potrebbe risultare di difficile gestione, dal momento che non sono fornite precise definizioni per quanto riguardo alcune caratteristiche fondamentali di questi sistemi; un approccio più ampio, e più coraggioso, al tema avrebbe potuto ricomprendere tutti i sistemi in grado di impattare in modo molto massiccio sulle attività umane e per i quali è previsto l'utilizzo di un codice informatico. Al momento, possiamo invece aspettarci discussioni sulle aree più di confine riguardo a cos'è un SIA al fine di evitarne le maglie legislative.

La difficoltà di non adottare una definizione più chiara in tal senso è probabilmente legata allo scopo estremamente ampio del regolamento così come ideato, rivolto a SIA utilizzati in settori diversissimi tra loro. Il sistema penale, andando ad incidere per sua natura in maniera invasiva su diritti fondamentali degli individui, è però un sistema peculiare nel contesto delle discussioni attorno all'uso – o al cattivo uso – dell'IA, con la conseguenza che la bozza così concepita lascia aperti molti dubbi circa la sua applicazione in tale ambito, specialmente considerando lo spazio abbondante previsto per eccezioni che lo riguardano direttamente (ad esempio con riferimento alle pratiche biometriche, o a tecnologie di sorveglianza di massa).

4.2. *Criticità di applicazione.*

Vi sono innanzitutto delle potenziali criticità di applicazione dovute ad alcune falle nel regolamento, che non considerano appieno ad esempio il ruolo dei privati nella gestione di certi ambiti di rilevanza penalistica – ruolo crescente in certi ordinamenti in contesti di privatizzazione o *multi-agency*[36]. Un breve esempio: nell'ambito dei SIA proibiti, è certamente positivo che non possano essere utilizzati sistemi di punteggio sociale che vadano a cercare

[35] In senso critico si sono espressi molti interventi apparsi sulla stampa specializzata, si veda ad esempio Chiusi (2021) e Clarke (2021).
[36] Si consideri ad esempio Byrne *et al.* (2019); Corda e Lagerson (2020).

pattern e modelli nella raccolta massiva di dati dei cittadini; tale analisi, infatti, nulla dovrebbe avere a che fare con la giustizia penale, specialmente in fase di prevenzione del crimine. Si noti però che la possibilità di attribuzione di un punteggio sociale ai cittadini che tanto ha allertato l'opinione pubblica (si pensi al caso cinese emerso negli ultimi anni e subito paragonato agli scenari distopici di *Black Mirror*[37]) risulta vietata soltanto nel settore pubblico: allo stato del tenore letterale della proposta, non appare vietata la possibilità per i privati di profilare e creare algoritmi di *social scoring* per le più disparate attività, e il dubbio al momento resta aperto circa la possibilità di utilizzo di tali sistemi in contesti di crescente privatizzazione della giustizia penale[38].

Come menzionato sopra, anche le ampie eccezioni previste di diretta rilevanza per l'ambito penalistico creano molti dubbi riguardanti la potenziale applicazione del Regolamento, qualora approvato nella sua formula attuale. Abbiamo visto ad esempio nella sezione 3.1 come siano previste una serie di eccezioni ai SIA proibiti (si pensi all'identificazione facciale) in ambito investigativo, alla luce di principi come quello di proporzionalità. Si tratta principalmente di situazioni in cui altri diritti vanno ad essere posti in bilanciamento con le necessità di privacy e dignità dell'individuo, come ad esempio nel caso della possibilità di ritrovare persone e bambini scomparsi. È certamente meritorio e condivisibile il bilanciamento operato; tale attenzione è senz'altro un segno di centralità della persona, al punto da rendersi necessario un sacrificio in termini di privacy alla collettività. Questa attenzione alla persona però sembra scontrarsi con la mancata considerazione ai problemi accertati che certi SIA soffrono con riferimento, per esempio, al riconoscimento automatico di individui appartenenti a minoranze etniche, col risultato che questo bilanciamento di interessi rischia di colpire di più, ancora una volta, determinati segmenti della popolazione. Del resto, la bozza non richiede alcuna garanzia in tal senso.

Con riferimento ai SIA proibiti, molto problematica potrebbe essere anche l'applicazione della terza eccezione all'uso del riconoscimento facciale, quella che fa riferimento ad una certe gravità del reato per cui si procede (ovvero alla pena detentiva di minimo tre anni) come discrimine per permettere un'eccezione a fini investigativi, e che potrebbe portare a importanti diversità e disparità di trattamento in presenza di diverse qualificazioni di reati e diversi regimi edittali nei vari Stati Membri, con conseguenti complicazioni anche in un'ottica di cooperazione di polizia e giudiziaria: vi è il rischio che una tipologia di SIA sia operativa in uno Stato, mentre non sia ammessa in un altro, pur all'interno dell'Unione Europea e per la medesima fattispecie.

Nel complesso, queste eccezioni potrebbero scardinare molto dell'impianto del Regolamento, a seconda di come verranno interpretate e implementate, dal momento che potrebbero permette re un'ampia casistica di riconoscimento facciale in ambito penalistico per individuare e isolare singoli individui in contesti pubblici. Tale "estrapolazione dalla folla" è tuttavia problematica, come evidenziato nei casi di Hong Kong e delle proteste negli Stati Uniti d'America[39]. Sarà certamente oggetto di dibattito nel corso dei prossimi mesi cercare di mantenere tale eventualità al di fuori delle condotte ammesse dal Regolamento, pena l'abbandono di qualsiasi rilevanza della categoria oggi proposta come rischio inaccettabile.

Un altro punto di criticità importante riguarda la relazione tra le categorie proposte. Paradossalmente, per i SIA ricompresi nella categoria "ad alto rischio" non ritroviamo alcuni degli oneri previsti per SIA di categoria inferiore (come ad esempio i *chatbox*). Sembra infatti che la necessità di avere piena consapevolezza di stare interagendo con un SIA sia stata prevista soltanto per profili di basso rischio, in quanto chiamati ad operare senza intermediazione di utenti professionali. Se, certamente, è apprezzabile che l'utente chiamato a interagire con un'intelligenza artificiale "a basso rischio" abbia la conoscenza e la conoscibilità di stare interagendo con una macchina (anche, ad esempio, vedendo un video generato con *deepfake*), non sembra ugualmente replicata la previsione per i SIA "ad alto rischio". In tali casi, è infatti prevista l'interposizione di figure professionali che possono agire, controllare, aggiustare ed eventualmente rivedere (anche senza tenerne conto) la scelta dell'intelligenza artificiale (art.

[37] Si veda ad esempio Parlangeli (2017). Cfr. anche Pieranni (2020).
[38] Fitzgibbon e Lea (2018).
[39] L'abilità di un SIA di riconoscere un volte tra una molteplicità di persone è certamente molto utile in caso di ricerca di una persona specifica all'interno di una folla, ma può portare alla criminalizzazione e alla sanzione di un singolo individuo per un'attività collettiva, come ad esempio una manifestazione. In tal caso, l'intervento del SIA costituisce un elemento che va a scardinare in modo evidente il quadro dei diritti individuali e collettivi di una società. Cfr. Millet (2020).

14). La conseguenza è però che, mentre un utente avrebbe da Regolamento sempre contezza di stare interagendo con un *chatbot* nel richiedere un'informazione online, lo stesso utente potrebbe non sapere mai che un SIA è stato determinante nel portare avanti un'investigazione a suo carico, o nella determinazione della sua pena in un procedimento giudiziario. Il disvelamento, tuttavia, condurrebbe ad un ulteriore problema: laddove l'intervento umano avvenga *in melius*, infatti, non si aprono spazi per alcuna contestazione; in caso, invece, di intervento *in peius*, chi ha disatteso il suggerimento del SIA si potrebbe trovare costretto ad argomentare il motivo della propria scelta, e tale condizione potrebbe non essere agevole dal momento che può essere impossibile da ricostruire appieno la motivazione della scelta del SIA[40].

4.3. *Criticità di spazio.*

i sono delle criticità inerenti alla dimensione transnazionale del problema: per avere successo, la proposta di Regolamento dovrà essere accettata come standard da altri attori principali nel panorama internazionale. Da un lato, Paesi terzi si troverebbero nella posizione di non potere ignorare un Regolamento Europeo sul tema per mantenere competitività a livello internazionale (indipendentemente dal fatto che internamente adottino regolamentazioni simili). Ad esempio, pur privo di effetti diretti nel Regno Unito post Brexit, un regolamento UE non potrebbe essere ignorato oltremanica, ed infatti la bozza ha già iniziato ad essere discussa nel settore[41], con particolare attenzione ai suoi effetti extraterritoriali (nel caso, ad esempio, una compagnia basata in un paese terzo offra SIA "ad alto rischio" ad un ente basato nell'Unione Europea). Si può ritenere, per alcuni profili, che lo sviluppo di IA all'interno dell'Unione potrebbe risultare "avvantaggiato" dalla possibilità di sviluppare una IA *compliant by default* con il Regolamento. Certamente sembra questo l'auspicio della Commissione, sia per aver divulgato il draft con anticipo, sia per aver impostato un percorso di co-regolamentazione dell'IA che intende ripercorrere analoghi percorsi (RGDP su tutti).

D'altro canto – ed è questa probabilmente la ragione alla base di una certa timidezza nell'approccio adottato nella bozza – vi è la paura che una regolamentazione troppo stringente possa fungere da disincentivo per aziende per sviluppare le loro tecnologie nei Paesi dell'Unione, inducendole a preferire ordinamenti con meno vincoli. Per esempio, l'approccio statunitense per il momento ha lasciato ampi spazi alle grandi aziende tecnologiche sul suo territorio; potrebbe non essere facile vincere la resistenza di queste grosse aziende (si pensi a Google, Amazon e le grosse *social media companies*) che fanno ampio uso di SIA, ma soprattutto possiedono quantità incredibili di dati, necessari per fare funzionare molti di questi sistemi.

Un ulteriore profilo di interesse riguarda i SIA e di come necessariamente debbano andare a coordinarsi con norme penali, all'interno dello spazio europeo, che presentano notevoli profili di diversità. Sarà necessario analizzare nel corso dei prossimi anni, in parallelo con la convergenza e l'armonizzazione delle legislazioni in materia, come le disposizioni del Regolamento potranno impattare sulla vita di tutti i giorni dei sistemi penali europei. Da quanto emerge dalla bozza, sembra lecito aspettarsi che possa verificarsi, infatti, il caso in cui una previsione differente tra due Stati consenta di autorizzare in uno di essi l'utilizzo di un determinato SIA, mentre lo stesso SIA potrebbe rimanere vietato nell'altro Stato, pur nell'ambito della medesima fattispecie. Tale possibilità è certamente contemplata dalla proposta del Regolamento, ma si presta ad aprire ampi margini di differenziazione all'interno dell'Unione.

Per quanto riguarda specificamente SIA di diretta rilevanza per il sistema penale, la proposta di regolamentarli in Europa è comunque da accogliere con particolare favore nel momento in cui essa può costituire un freno all'ingresso nel continente di software di diversa origine (generalmente americana o cinese) all'interno di uffici giudiziari e forze di polizia, cosa che potrebbe presentare gravi problematicità da un punto di vista della tutela dei diritti fondamentali, ma anche problemi di sicurezza non indifferenti. L'ingresso di tali soluzioni in posizioni critiche per l'intero ecosistema di pesi e contrappesi, diritti e responsabilità dell'Unione, costituisce una vulnerabilità non solo in termini di sovranità digitale, ma anche in termini di sicurezza informatica.

[40] *Ex multis*, Wisser (2019).
[41] Peeters *et al.* (2021).

4.4. *Criticità di tempo.*

Come discusso all'inizio di questo breve contributo, nell'ambito dei SIA vi è un vuoto normativo che permane da anni. Potrebbe volerci ancora molto tempo prima che la bozza qua discussa diventi provvedimento legislativo; potenzialmente anni, e la bozza stessa prevede un periodo di implementazione di 18 mesi prima della sua entrata in vigore. Rimane dunque, al momento, un importante profilo di criticità legato alle tempistiche di (potenziale miglioramento e) adozione di questo testo normativo, di fronte al crescente utilizzo di SIA anche in ambiti sensibili come quello della giustizia penale.

Il Regolamento ha affrontato il problema del suo futuro adattamento alla rapida evoluzione dei SIA con il sistema degli allegati. È questa una soluzione pratica, ma non esente da problemi: l'approccio a elencazione presente negli allegati, infatti, non elimina il problema dell'intervallo temporale che necessariamente si crea tra l'emersione di una nuova tecnologia o la sua implementazione, e l'aggiornamento dell'allegato di riferimento[42].

4.5. *Criticità di intervento.*

Il successo o meno della regolamentazione dei SIA è anche, da ultimo, connesso in modo molto diretto con l'ambito di intervento specifico e con il profilo sanzionatorio. A riguardo, si sono riproposti meccanismi simili a quelli usati per il RGDP, prevedendo questa volta multe fino al 6% del fatturato annuo per le aziende coinvolte o fino a 30 milioni di euro (art. 72). Dalla lettera della norma, tuttavia, sembra ridotto l'impatto della sanzione nel suo complesso, in quanto erogabile soltanto *una tantum* e non in modo proporzionale al numero delle singole violazioni o dei singoli danni arrecati dal SIA non conforme. Tale mancata previsione, adottata comprensibilmente per la difficoltà di accertare violazioni e danni concreti come invece nella protezione dei dati, impone di riflettere su quale possa essere in concreto l'effetto deterrente della proposta: in presenza di società dalle disponibilità estremamente ingenti, come le *big tech* che già oggi sviluppano sofisticati SIA (e SIA ancora più sofisticati potrebbero essere sviluppati in futuro), anche il limite di 30 milioni di euro potrebbe apparire insufficiente in vista del potenziale guadagno ottenibile sviluppando e utilizzando un SIA non completamente conforme. Lo sviluppo di SIA particolarmente avanzati, infatti, è appannaggio di grandi realtà, specialmente extra-europee, sulle cui disponibilità economiche dovrebbe essere parametrato un vero limite che sia responsabilizzante verso lo sviluppo di SIA correttamente individuati come "molto pericolosi".

La responsabilizzazione legale degli attori commerciali, in particolare nel settore tecnologico, è certamente ancora molto porosa: anche se la questione sta ricevendo un'attenzione crescente e vi è ormai una certa pressione politica per regolamentare meglio il settore, non vi è ancora un quadro giuridico internazionale coerente sul tema[43]. Del resto, intervenire per trovare nuovi equilibri tra la spinta verso la massimizzazione del profitto delle aziende tecnologiche e la difesa degli interessi della nostra società è probabilmente una delle principali sfide odierne.

Nel complesso, la proposta lascia troppa carta bianca alle imprese in termini di autoregolamentazione e non innova riguardo il profilo sanzionatorio (riproponendo le sole sanzioni economiche come strumento). A fronte di una così importante materia da normare, tuttavia, poteva essere l'occasione per introdurre sanzioni più variegate, ad esempio prevedendo sistemi di sospensione e *ban* per i SIA non rivelatisi conformi. Tali categorie di sanzioni sarebbero state in linea con l'intento innovativo della proposta, principalmente esplicatosi nella creazione della categoria del "rischio inaccettabile", e potrebbero rappresentare l'unica vera misura di deterrenza allo sviluppo di SIA "spregiudicati".

Specifiche criticità di intervento si rilevano anche riguardo a una possibile sproporzione normativa tra SIA ad alto rischio e SIA generici, così come riguardo alle troppe eccezioni che traspaiono dalle norme. Con riferimento al primo dei due problemi, è stato ripreso dalla disci-

[42] È questo un problema noto, ad esempio, nell'ambito della regolamentazione delle sostanze illecite in ambito internazionale, che ha dato adito all'intero problema delle *new psychotropic substances* (NPSs), ovvero sostanze che sfuggono alla regolamentazione in materia delle Nazioni Unite. Si veda sul punto il sito dell'European Monitoring Center for Drug and Drug Addition (https://www.emcdda.europa.eu/topics/nps_en).
[43] Cfr. Walker *et al.* (2000).

plina del RGDP il concetto di trasparenza: qualora il SIA interagisca o sia altresì rivolto direttamente ad individui (si pensi all'uso di dati biometrici, il riconoscimento facciale o l'uso di *deepfake*), l'utente interessato deve essere avvisato dell'utilizzo del SIA. L'utente, in altre parole, deve essere messo in grado di decidere se continuare a interagire col SIA, in alcuni casi potendo richiedere un intervento e un'interazione umana. Tale possibilità, tuttavia, espressamente prevista per SIA a basso rischio (art. 52), non è ugualmente prevista per SIA riconosciuti a rischio molto maggiore, potenzialmente creando una dannosa sproporzione normativa. In riferimento al secondo problema, le numerose eccezioni potrebbero prestare il fianco ad una difficile applicazione della norma e ad un proliferare di utilizzi ambigui. Tale frammentarietà della norma (si pensi, ad esempio, al riconoscimento facciale ammesso se autorizzato dall'autorità giudiziaria, o al *social scoring* generalmente autorizzato se realizzato da società private) può creare abusi, sfruttabili per conseguire vantaggi illeciti, condurre azioni criminali con la possibilità di non essere perseguiti, o impegnarsi in metodologie ibride di conflitto[44].

Va infine considerato come la proposta di regolamento non si applica ai SIA utilizzati esclusivamente per scopi militari (Considerando 12), o con riferimento alle autorità pubbliche di Paesi terzi o organizzazioni internazionali che utilizzino SIA sulla base di accordi internazionali (Considerando 11). Tali limitazioni sono comprensibili, esistendo una normativa specifica, ma certamente riducono l'impatto della proposta e non estendono al di fuori di essa, per il momento, quanto di positivo è invece stato sottolineato.

5. Conclusioni.

Alla luce delle considerazioni svolte, la proposta costituisce un buon punto di partenza per disciplinare l'IA. Il tentativo, seppur iniziale, di attribuire una responsabilità intorno ai SIA e di definire requisiti di trasparenza e limiti è essenziale per lo sviluppo sostenibile dell'ambiente digitale dei prossimi decenni. Per tale ragione, la normativa è quanto mai opportuna e, anzi, non deve tardare ulteriormente.

In questo contributo si sono descritti gli ambiti di intervento della proposta ed evidenziati i principali limiti che appaiono quando si faccia attenzione al versante penalistico e criminologico. Vi sono criticità di scopo e di applicazione che richiedono di essere analizzate, alla luce del pesante intervento della normativa proposta sulle normali attività di utilizzo dei SIA nel contrasto al crimine e nell'amministrazione della giustizia. Come si è cercato di evidenziare, sarà interessante capire come le molteplici "eccezioni", previste per finalità specifiche, andranno ad operare nella realtà concreta e come il Regolamento nel suo complesso ne verrà condizionato. Mentre si cominciano a raccogliere i frutti di alcune delle normative riguardanti il digitale, come ad esempio il RGDP, a distanza di qualche anno dalla piena applicazione, per altre già si avverte il bisogno di un prematuro intervento volto a correggere la rotta (su tutte, la Direttiva NIS). Nel caso di questa proposta, la risoluzione di alcuni dei profili di criticità più rilevanti prima del varo del testo definitivo potrebbe essere fondamentale per disciplinare un settore vitale come quello dell'IA.

Il Regolamento andrà a ridefinire oneri e obblighi dei produttori di SIA, così come a modificare alcuni casi dell'interazione tra utenti e SIA. La maggiore consapevolezza riguardo questi utilizzi potrebbe portare ad una migliore comprensione dell'ambiente digitale dei prossimi anni, ma non si può escludere che, in realtà, il Regolamento non basti e sia di per sé insufficiente. Le previsioni, infatti, potrebbero non bastare a scongiurare il rischio di *techlash* legato all'AI, ovvero la reazione avversa alle nuove tecnologie che è generalmente causata dalla mancanza di fiducia nei confronti:

i) delle tecnologie stesse (ad esempio, perché rimangono delle *black box* anche a sempre maggiore impatto e pervasività); *ii*) di chi opera attraverso le tecnologie (sia esso produttore o utilizzatore); *iii*) di chi è chiamato a "certificare" le tecnologie o controllare l'operato degli attori coinvolti. Tutti questi tre ambiti sono direttamente coinvolti dalla proposta di Regolamento e presentano specifiche criticità (ad esempio, riguardo spazio e tempo, ma anche intervento). Il compito non semplice di regolamentare per la prima volta un settore innovativo,

[44] Ovvero metodologie di conflitto che prevedono l'utilizzo simultaneo di approcci convenzionali e non convenzionali. *In primis*, si pensi, ad esempio, alle "minacce ibride", ormai considerate una categoria concettuale fondamentale in relazione alla conflittualità nell'infosfera, cfr. Sari (2019 e 2020).

come certamente è quello dell'IA, ben può richiedere l'introduzione di concetti nuovi (come la previsione del "rischio inaccettabile") e potrebbe richiedere l'implementazione di strumenti nuovi (come le sanzioni a tempo, che nel presente lavoro sono state proposte), tale è la capacità di controllare aspetti importanti delle nostre vite tramite l'uso di SIA.

Nel complesso, da un punto di vista di contrasto alla criminalità sono evidenti le limitazioni poste in essere nei confronti delle forze di polizia e delle autorità pubbliche, che non possono generalmente utilizzare avanzati SIA in molte delle loro attività. Il timore che il cittadino sia esposto ad abusi da parte dell'autorità pubblica tramite un SIA, e sui quali ha poco o nessun controllo, porta a comprendere le ragioni di tale limitazione. Come evidenziato, tuttavia, permangono ambiti molto ampi in cui un SIA si troverà ad essere utilizzato anche dall'autorità pubblica senza che il cittadino presumibilmente ne venga pienamente a conoscenza (si pensi, ad esempio, ad un sistema di calcolo della pena o della recidiva). Ancora più ampi sono gli spazi lasciati liberi al privato (ovvero, alle grandi società del digitale) per poter operare senza trasparenza nei confronti degli utenti.

Le limitazioni poste in essere nei confronti delle forze di polizia e delle autorità pubbliche conducono anche ad una seconda considerazione: il divieto di utilizzare strumenti evoluti potrebbe ridursi nel perpetuare l'utilizzo di strumentazioni e di metodologie ancora meno precise, ad esempio per elaborare profili e strategie di contrasto alla criminalità. Un SIA, infatti, in casi specifici potrebbe meglio dell'essere umano andare a definire *cluster* all'interno del medesimo gruppo sociale, ad esempio evidenziando differenze non percepibili all'occhio umano ed evitando che il medesimo trattamento sia riservato a tutti gli appartenenti di un gruppo in ragione di un pregiudizio umano. Come chiaramente mostrato negli ultimi anni, l'IA ben può assolvere a determinati compiti per i quali la potenza di calcolo di un computer è certamente più idonea dell'attività umana, come ad esempio il riconoscimento di pattern comportamentali su grandi numeri o la definizione di *cluster*. Ciò potrebbe permettere l'elaborazione di migliori strategie di contrasto al fenomeno criminale, in ragione di elementi difficilmente analizzabili e quantificabili senza un ausilio computazionale sofisticato; parimenti, l'uso di specifici SIA, opportunamente disciplinati e controllati, potrebbe portare a comportamenti più responsabili e meno discriminatori da parte delle forze dell'ordine stesse. Il problema alla base rimane quello dei limiti dei dati sui quali l'IA viene "addestrata", e l'esplicito riconoscimento dei limiti dei SIA prima e durante la loro messa in uso per evitare distorsioni – ma queste sono problematiche sulle quali la bozza di Regolamento, sfortunatamente, non va ad incidere.

Bibliografia

Aghababei, Sommayyeh e Makrechi, Masoud (2018): "Mining Twitter data for crime trend prediction", *Intelligent Data Analysis*, 22(1), pp.117-141.

Angwin, Julia e Larson, Jeff (2016); "Bias in criminal risk scores is mathematically inevitable, researchers say". Disponibile all'indirizzo: https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say.

Barocas, Solon e Selbest, Andrew D. (2016): "Big data's disparate impact", *California Law Review*, 104, pp.671-732.

Becker, Howard S. (1963): *Outsiders: studies in the sociology of deviance*, New York, Free Press.

Benanti, Paolo (2018): *Oracoli. Tra algoretica e algocrazia*, Roma, Luca Sossella editore.

Benanti, Paolo (2020): *Digital Age*, Edizioni San Paolo.

Bennet Moses, Lyria e Chan, Janet (2018): "Algorithmic prediction in policing: Assumptions, evaluations, and accountability", *Policing and Society,* 28(7), pp.806-822.

Brkan, Maja (2019): "Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond", *International Journal of Law and Information Technology*, 27(2), pp.91-121.

Byrne, James, Kras, Kimberly R. e Marmolejo, Lina M. (2019): "International perspectives on the privatization of corrections", *Criminology and Public Policy*, 18, pp.477-503.

Celotto, Alfonso (2019): "Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto", in *Analisi Giuridica dell'Economia, Studi e discussioni sul diritto dell'impresa*, 1, pp.47-60.

Cevolini, Alberto e Esposito, Elena (2020): "From pool to profile: Social consequences of algorithmic prediction in insurance", *Big Data & Society*, 7(2).

Chan, Janet e Bennet Moses, Lyria (2015): "Is big data challenging criminology?", *Theoretical Criminology*, 20(1), pp.21-39.

Chiusi, Fabio (2021): "La proposta UE per regolamentare l'intelligenza artificiale: un testo che potrebbe cambiare la storia o quasi nulla". ValigiaBlu.it. Disponibile all'indirizzo: https://www.valigiablu.it/intelligenza-artificiale-proposta-ue/.

Cioffi, Raffaele, Travaglioni, Marta, Piscitelli, Giuseppina, Petrillo, Antonella e De Felice, Fabio (2020): "Artificial Intelligence and Machine Learning Applications in Smart Production: Progress, Trends, and Directions", *Sustainability*, 12, p.492

Clarke, Laurie (2021): "The EU's leaked AI regulation is ambitious but disappointingly vague". TechMonitor.ai. Disponibile all'indirizzo: https://techmonitor.ai/policy/eu-ai-regulation-machine-learning-european-union.

Cohen, Julie E. (2019): *Between Truth and Power: The Legal Constructions of Information Capitalism*, Oxford, Oxford University Press.

Commissione Europea (2018): *Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni: L'intelligenza artificiale per l'Europa*, COM(2018) 237.

Commissione Europea (2021a): *Proposta per un Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale*, COM(2021) 206 final. Disponibile al seguente indirizzo: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence.

Commissione Europea (2021b): *Comunicazione sullo sviluppo di un approccio Europeo all'Intelligenza Artificiale*. Disponibile all'indirizzo: https://digital-strategy.ec.europa.eu/en/library/communication-fostering-european-approach-artificial-intelligence.

Corda, Alessandro e Lagerson, Sarah E. (2020): "Disordered Punishment: Workaround Technologies of Criminal Records Disclosure and the Rise of a New Penal Entrepreneurialism", *The British Journal of Criminology*, 60(2), pp.245-264.

Custers, Bart H.M. (2013) "Data Dilemmas in the Information Society", in Custers, Bart H.M, Calders, Toon, Schermer, Bart e Zarsky, Tal (editors) *Discrimination and Privacy in the Information Society,* Heidelberg, Springer.

Dubber, Markus D., Pasquale, Frank e DAS, Sunit (editors) (2020): *The Oxford Handbook of Ethics of AI*, Oxford, Oxford University Press.

Eaglin, Jessica (2017): "Constructing Recidivism Risk", *Emory Law Journal*, pp.59-122.

Ensign, Danielle, Friedler, Sorelle A., Neville, Scott, Scheidegger, Carlos e Venkatasubramanian, Suresh (2018): "Runaway feedback loops in predictive policing", Machine Learning Research. Conference on Fairness, Accountability, and Transparency, 81, pp.1-12.

Esposito, Elena (2013): "Digital prophecies and web intelligence", in Hildebrandt, Mirelle e De Vries, Katja (editor): *Privacy, Due Process and the Computational Turn*, Londra, Routledge.

Ferguson, Andrew G. (2012): "Predictive policing and reasonable suspicion", Emory Law Journal, 62, pp.259-325.

Ferguson, Andrew G. (2017): *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement,* New York, New York University Press.

Finocchiaro, Giusella (2019): "Intelligenza artificiale e protezione dei dati personali", *Giurisprudenza Italiana*.

Fitzgibbon, Wendy e Lea, John (2018): "Privatization and coercion: The question of legitimacy", *Theoretical Criminology*, 22(4), p.545-562.

Fussey, Pete e Murray, Daragh (2019): *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*.

Gruetzemacher, Ross e Whittlestone, Jess (2019): "Defining and Unpacking Transformative AI", arXiv:1912.00747v2.

Hamilton, Melissa (2015): "Risk-Needs Assessment: Constitutional and Ethical Challenges", *American Criminal Law Review,* 231, pp.236-239.

Hannah-Moffat, Kelly (2018): "Algorithmic Risk Governance: Big Data Analytics, Race and Information Activism in Criminal Justice Debates", *Theoretical Criminology*, 1-18.

Harcourt, Bernard E. (2015): "Risk as a proxy for race", *Federal Sentencing Reporter*, 27, pp.237-243.

Hao, Karen e Stray, Jonathan (2019): "Can you make AI fairer than a judge? Play our courtroom algorithm game", *MIT Technology Review*.

Hardns, Wim e Rummens, Anneleen (2017): "Predictive policing as a new tool for law enforcement? Recent developments and challenges", *European Journal of Criminal Policy and Research*, 24(3), pp.201-218.

Iliadis, Andrew e Russo, Federica (2016): "Critical data studies: An introduction", *Big Data & Society*, 3(2), pp.1-7.

International Technology Law Association (2019/2021): *Responsible AI*. Disponibile all'indirizzo: https://www.itechlaw.org/ResponsibleAI2021.

Jasanoff, Sheila (2015): "Future imperfect: Science, technology, and the imaginations of modernity", in Jasanoff, Sheila e Kim, Sand Hyun (editors) *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power,* Chicago, University of Chicago Press.

Kearns, Michael e Roth, Aaron (2020): *The Ethical Algorithm,* Oxford, Oxford University Press.

Lavorgna, Anita (2020): *Cybercrimes. Critical issues in a global context,* Londra, MacMillan.

Lavorgna, Anita, Middleton, Stuart E., Pickering, Brian e Neumann, Geogg (2020): "FloraGuard: tackling the online trade in endangered plants through a cross-disciplinary ICT-enabled methodology", *Journal of Contemporary Criminal Justice*, 36(3), pp.428-450.

Lavorgna, Anita e Uwgudike, Pamela (2021): "The datafication revolution in criminal justice: An empirical exploration of frames portraying data-driven technologies for crime prevention and control" (in revisione).

Law Society (2019): *Algorithm Use in the Criminal Justice System Report*. Disponibile all'indirizzo: https://www.lawsociety.org.uk/support-services/research-trends/algorithm-use-in-the-criminal-justice-system-report.

Lombardi-Vallauri, Luigi (2017): "Algoretica: le due sfide cruciali nell'era tecnologica: bioetica, roboetica", in Olschki, Leo S., *Atti e memorie dell'Accademia toscana di scienze e lettere La Colombaria*, p.68.

Lum, Kristian e Isaac, William (2016): "To Predict and Serve?", *Significance*, 13, pp.14-19.

Mcstay, Andrew e Rosner, Gilad (2021): "Emotional artificial intelligence in children's toys and devices: Ethics, governance and practical remedies", *Big Data & Society*, doi:10.1177/2053951721994877.

Meyer, Chris, Cohen, David e Nair, Sudhir (2020): "From automats to algorithms: the automation of services using artificial intelligence", *Journal of Service Management*, 2020, 31(2), pp.145-161.

Middleton, Stuart E, (2021): "Use of Artificial Intelligence to support cybercrime research", in Lavorgna, Anita e Holt, Tom J. (editors) *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches*, Londra, Palgrave.

Millet, Tatum (2020): "A Face in the Crowd: Facial Recognition Technology and the Value of Anonymity", *Columbia Journal of Transnational Law*.

ISE (2020): Proposte per una Strategia italiana per l'intelligenza artificiale. Disponibile all'indirizzo: https://www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf.

NIST (2020/2021): *Four Principles of Explainable Artificial Intelligence*. Disponibile all'indirizzo: https://www.nist.gov/artificial-intelligence/ai-foundational-research-explainability.

Oswald, Marion, Grace, Jamie, Urwin, Sheena e Barnes, Geoffrey (2018): "Algorithmic risk assessment policing models: lessons from the Durham HART model and "experimental" proportionality", *Information & Communications Technology Law*, 27(2), pp.223-250.

Parlangeli, Diletta (2017): "La Cina darà un punteggio social ai suoi cittadini dal 2020". Wired.it. Disponibile all'indirizzo: https://www.wired.it/internet/web/2017/10/25/cina-punteggio-social-ai-cittadini-2020/?refresh_ce=.

Peeters, Michael, AIR, Christopher, Halford, Charlotte e Gilbert, Jack (2021): "The draft AU AI Regulation". Disponibile all'indirizzo https://www.dacbeachcroft.com/en/articles/2021/april/the-draft-eu-ai-regulation-what-you-need-to-know/.

Pieranni, Simone (2020): *Red Mirror,* Roma, Laterza.

Prinsloo, Paul (2020): "Of 'black boxes' and algorithmic decision-making in (higher) education – A commentary", *Big Data & Society*, doi:10.1177/2053951720933994.

Sari, Aurel (2019): "Legal Resilience in an Era of Gray Zone Conflicts and Hybrid Threats", in *Exeter Centre for International Law Working Paper*.

Sari, Aurel (2020): "Hybrid CoE Trend Report 3: Hybrid threats and the law: concepts, trends and implications", European Centre of Excellence for Countering Hybrid Threats.

Shapiro, Aaron (2017): "Reform predictive policing", *Nature*, 541(7638), pp.458-460.

Smith, Gavin J.d., Bennet Moses Lyria e Chan, Janet (2017): "The challenges of ding criminology in the big data era: towards a digital and data-driven approach", *British Journal of Criminology*, 57(2), pp.259-274.

Starr, Sonja B. (2014): "Evidence-based sentencing and the scientific rationalization of discrimination", *Stanford Law Review*, 66(4), pp.803-872.

Van Dijk, Johannes (2005): *The deepening divide: Inequality in the information society*, Thousand Oaks, Sage.

Villalba, Jorge F. (2020): "Algor-ética: la ética en la inteligencia artificial", *Anales De La Facultad De Ciencias Juridicas Y Sociales De La Universidad Nacional De La Plata*, 50, p.62.

Ubertis, Giulio (2020): "Intelligenza artificiale, giustizia penale, controllo umano significativo", *Diritto Penale Contemporaneo*, 4, pp.75-90.

Ugwudike, Pamela (2020): "Digital prediction technologies in the justice system: The implications of a 'race-neutral' agenda", *Theoretical Criminology*, 1-19.

Wachter, Sandra, Mittlestadt, Brent D. e Floridi, Luciano (2017): "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation", *International Data Privacy Law*, 7(2), pp.76-99.

Walker, Clive, Wall, David e Akdeniz, Yaman (2000): "The Internet, law and society", in Akdeniz, Yaman, Walker, Clive e wall, David (editors), *The Internet, Law and Society,* Harlow, Pearson.

Williams, Matthew, Burnap, Pete e Sloan, Luke (2017): "Crime sensing with big data: the affordances and limitations of using open-source communications to estimate crime patterns", *British Journal of Criminology,* 57(2), pp.320-340.

Wisser Leah (2019): "Pandora's Algorithmic Black Box: The Challenges of Using Algorithmic Risk Assessments in Sentencing", *American Criminal Law Review*, v. 56(4), 1-22.

Završnik, Aleš (ed.) (2018): *Big Data, Crime and Social Control*, Londra, Routledge.

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

http://dpc-rivista-trimestrale.criminaljusticenetwork.eu