Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

1/2020

Editore Associazione "Progetto giustizia penale", via Altaguardia 1, Milano - c.f. 97792250157
ANNO 2020 - 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.

Se desideri proporre una pubblicazione alla nostra rivista, invia una mail a 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

Responsabilità penale e principi del sistema

Responsabilidad penal y principios del sistema

Criminal Liability and System Principles

Appunti per una giustificazione liberale della pena 1
Argumentos para una justificación liberal de la pena
Notes on the Libertarian Ground of Criminal Penalty
Giovanni Cocco

Irretroattività e libertà personale: l'art. 25, secondo comma, Cost., rompe gli argini dell'esecuzione penale 22
Irretroactividad y libertad personal: el artículo 25, inciso segundo, de la Constitución rompe los diques de la "ejecución penal"
Irretroactivity and Personal Freedom: art. 25, 2nd para., of the Italian Constitution Breaks the Barriers of Penal Execution
Vittorio Manes e Francesco Mazzacuva

Così è (se vi pare) 45
Alla ricerca del volto dell'illecito penale, tra legge indeterminata e giurisprudenza imprevedibile
Así es (si les parece)
A la búsqueda del rostro del ilícito penal, entre leyes indeterminadas y jurisprudencia imprevisible
So It Is (If You Like)
Looking for the Criminal Provision Face, between Uncertain Legal Texts and Unforeseeable Case-Law
Federico Consulich

L'influsso dei precedenti europei sulla legge processuale nazionale 88
La influencia de los precedentes europeos sobre la ley procesal nacional
The Influence of European Precedents on Procedural National Law
Marcello Daniele

Il *nemo tenetur se detegere* nel labirinto delle fonti. 108
El* nemo tenetur se detegere *en el laberinto de las fuentes.
The* nemo tenetur se detegere *Principle in the Labyrinth of Law Sources.
Sofia Confalonieri

Contents

L'obiettivo su…

Objetivo sobre…

Focus On…

Le dichiarazioni fraudolente: fattispecie da ripensare? 142
Las declaraciones fraudulentas: ¿un delito para repensar?
Fraudulent Tax Returns: Criminal Provisions to Be Rethought?
Francesco Mucciarelli

L'esercizio abusivo della professione riformato. Il caso dell'attività odontoiatrica 162
El delito de ejercicio ilegal de la profesión. El caso de la actividad odontológica
The Crime of Unlicensed Practice after the Reform. The Case of Dentistry
Matteo Caputo

L'unificazione di traffico di influenze e millantato credito: una crasi mal riuscita 188
La unificación del tráfico de influencias y del "millantato credito": una fusión mal concebida
The Unification of Trading in Influence and Influence Peddling: a Failed Mix
Pierpaolo Astorina Marino

State Terrorism as Human Rights Infringement, Particularly in the Involvement of State Agents 200
Terrorismo di Stato come violazione dei diritti umani, con particolare riferimento al coinvolgimento di agenti statali
El Terrorismo de Estado como violación a los Derecho Humanos. En especial la intervención de los agentes estatales
Raúl A. Carnevali

Lo sbarco del *taser* in Italia: i diritti (non) presi sul serio 218
El desembarco del **taser** *en Italia: Los derechos (no) tomados en serio*
The Taser lands in Italy: Taking Rights (Not) Seriously
Rosa Anna Ruggiero

Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della *High Court of Justice* 231
Novedades desde el Reino Unido: Reconocimiento facial aprobado por la **High Court of Justice**
News From the UK: Facial Recognition Approved by the High Court of Justice
Jacopo Della Torre

Diritto penale e "culto del littorio" 248
Derecho Penal y culto al fascismo
Criminal Law and 'Fascism Cult'
Dora Tarantino

L'obiettivo su...
Objetivo sobre...
Focus On...

142 **Le dichiarazioni fraudolente: fattispecie da ripensare?**
Las declaraciones fraudulentas: ¿un delito para repensar?
Fraudulent Tax Returns: Criminal Provisions to Be Rethought?
Francesco Mucciarelli

162 **L'esercizio abusivo della professione riformato. Il caso dell'attività odontoiatrica**
El delito de ejercicio ilegal de la profesión. El caso de la actividad odontológica
The Crime of Unlicensed Practice after the Reform. The Case of Dentistry
Matteo Caputo

188 **L'unificazione di traffico di influenze e millantato credito: una crasi mal riuscita**
La unificación del tráfico de influencias y del "millantato credito": una fusión mal concebida
The Unification of Trading in Influence and Influence Peddling: a Failed Mix
Pierpaolo Astorina Marino

200 **State Terrorism as Human Rights Infringement**
Terrorismo di Stato come violazione dei diritti umani
El Terrorismo de Estado como violación a los Derecho Humanos.
Raúl A. Carnevali

218 **Lo sbarco del *taser* in Italia: i diritti (non) presi sul serio**
El desembarco del* taser *en Italia: Los derechos (no) tomados en serio
The Taser lands in Italy: Taking Rights (Not) Seriously
Rosa Anna Ruggiero

231 **Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della *High Court of Justice***
***Novedades desde el Reino Unido: Reconocimiento facial aprobado por la* High Court of Justice**
News From the UK: Facial Recognition Approved by the High Court of Justice
Jacopo Della Torre

248 **Diritto penale e "culto del littorio"**
Derecho Penal y culto al fascismo
Criminal Law and 'Fascism Cult'
Dora Tarantino

Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della *High Court of Justice*

Novedades desde el Reino Unido: Reconocimiento facial aprobado por la High Court of Justice

News From the UK: Facial Recognition Approved by the High Court of Justice

Jacopo Della Torre
Dottore di ricerca in Scienze giuridiche presso l'Università degli Studi di Trieste e l'Università degli Studi di Udine
jdellatorre@units.it

Privacy | Pivacidad | Privacy

Abstracts

L'autore analizza una recente sentenza della *High Court of Justice* dell'Inghilterra e Galles, la quale è stata, a più voci, presentata come la prima decisione giudiziale a livello globale ad aver affrontato, in modo analitico, la tematica della compatibilità con il diritto alla riservatezza dell'utilizzo da parte delle forze di polizia di *software* di riconoscimento facciale. Pur non essendo riuscita a sedare l'acceso contrasto britannico tra sostenitori e detrattori dei *facial recognition systems*, siffatta pronuncia presenta aspetti di grande interesse anche per l'ordinamento italiano, nel quale gli strumenti in questione sono in dotazione alle autorità di *law enforcement*, ma non hanno una regolazione normativa soddisfacente.

El trabajo analiza la reciente sentencia de la High Court of Justice de Inglaterra y Gales, la cual ha sido descrita por muchos como la primera decisión judicial que aborda analíticamente la cuestión sobre la compatibilidad del uso de las herramientas de reconocimiento facial por parte de la autoridad y el derecho a la privacidad. A pesar de que la sentencia no fue capaz de resolver el conflicto entre defensores y detractores de los sistemas de reconocimiento facial, ella plantea cuestiones de gran interés para el sistema italiano, en el cual tales herramientas se encuentran a disposición de la autoridad pero sin una suficiente regulación.

This paper analyses a recent judgment by the High Court of Justice of England and Wales, described by many commentators as the first judicial decision worldwide to deal analytically with the issue of compatibility between the usage of facial recognition tools by law enforcement on the one hand and the right to privacy on the other. Although the judgment has not solved the tensions between supporters and opponents of facial recognition systems in the UK, it has raised issues of great interest even for the Italian legal system, where such tools are available to law enforcement agencies but are not sufficiently regulated by law.

Sommario 1. Premessa. – 2. Il progetto pilota della *South Wales Police* in tema di riconoscimento facciale. – 3. La decisione della *High Court*. – 4. Le reazioni critiche alla pronuncia della Corte. – 5. Qualche (breve) notazione conclusiva riguardante l'Italia.

1. Premessa.

Negli ultimi tempi, la discussione concernente l'impiego nella giustizia penale di dispositivi tecnologici, basati su sistemi di "intelligenza artificiale" (d'ora innanzi IA), si è arricchita di un novero di contributi davvero ampio[1]. All'interno di questo ricco filone, uno dei profili maggiormente controversi riguarda l'utilizzo da parte delle autorità di *law enforcement* di vari Paesi extraeuropei[2] ed europei[3] (tra cui, merita precisarlo fin da subito, vi è anche l'Italia[4]) di *software* di "riconoscimento facciale"; ossia *tools* che consentono di associare alla foto o al video di un volto di uno sconosciuto una o più immagini, contenute in una banca dati di dimensioni variabili, di soggetti le cui generalità siano già note[5]. I cd. *facial recognition systems* operano, più precisamente, mediante algoritmi, in grado di rilevare «le cosiddette impronte facciali (*face-print*), ovvero un certo numero di tratti, quali la posizione degli occhi, del naso, delle narici, del mento, delle orecchie e per il loro tramite [di] elabora[re] un modello biometrico finalizzato al riconoscimento»[6].

Si tratta di strumenti tecnici potenzialmente idonei a fornire un ausilio importante nell'attività di prevenzione e repressione della criminalità[7]. Essi sono in grado, infatti, non solo di identificare in modo più rapido persone di cui non si conosca l'identità, ma anche di conoscere in tempo reale se un certo individuo, sospettato di aver compiuto (o di poter commettere) un reato[8], possa trovarsi in un determinato luogo, sottoposto a osservazione. Laddove un *software* di riconoscimento facciale operi in modalità *real-time*, esso consente, infatti, di analizzare in

[1] Tra i più recenti contributi in lingua italiana pubblicati sul tema, cfr. Barbaro (2018), pp. 189 ss.; Basile (2019); Contissa *et. al* (2019), pp. 619 ss.; Costanzi (2018), pp. 166 ss.; D'Agostino (2019), pp. 354 ss.; Gialuz (2019); Maldonato (2019), pp. 401 ss.; Nieva-Fenoll (2019); Occhiuzzi (2019), pp. 391 ss.; Parodi e Sellaroli (2019); Quattrocolo (2019b), pp. 1 ss.; Ead. (2019c), pp. 135 ss.; Ead. (2019d), pp. 1748 ss.; Ead. (2018); Riccio (2019); Traversi (2019); Ziroldi, (2019). In lingua inglese, si vedano, perlomeno, Pagallo e Quattrocolo (2018), pp. 385 ss.; Quattrocolo (2019a), 1519 ss. e Završnik (2018), ai quali si rinvia anche per ulteriori riferimenti dottrinali in lingua straniera.

[2] Ci si riferisce, ad esempio, alla Cina (Li e Cadell, *China eyes "black tech" to boost security as parliament meets*, in *www.reuters.com*, 10 marzo 2018; Mozur e Krolik, *A Surveillance Net Blankets China's Cities, Giving Police Vast Powers*, in *www.nytimes.com*, 17 dicembre 2019), all'India (v. Toussaint, *Indian police are using facial recognition to identify protesters in Delhi*, in *www.fastcompany.com*, 30 dicembre 2019; Zaugg, *India is trying to build the world's biggest facial recognition system*, in *edition.cnn.com*, 18 ottobre 2019), alla Russia (Vincent, *Moscow rolls out live facial recognition system with an app to alert police*, in *www.theverge.com*, 30 gennaio 2020) e agli Stati Uniti (Brandom, *Police are using facial recognition the wrong way. And altering our faces?*, in *www.theverge.com*, 26 luglio 2019; Collins, *Facial recognition: Do you really control how your face is being used?*, in *eu.usatoday.com*, 23 dicembre 2019; Hamann e Smith, *Facial Recognition Technology: Where Will It Take Us?*, in *www.americanbar.org*; Garvie, Bedoja, Frankle, *The perpetual line-up. Unregulated police face recognition in America*, in *https://www.perpetuallineup.org/*, 18 ottobre 2016; Garvie e Moy, *America under Watch. Face surveillance in the United States*, in *https://www.americaunderwatch.com/*, 16 maggio 2019; Shuppe, *How facial recognition became a routine policing tool in America*, in *www.nbcnews.com*, 11 maggio 2019; Valentino-DeVries, *How the Police Use Facial Recognition, and Where It Falls Short*, in *www.nytimes.com*, 12 gennaio 2020). È bene, peraltro, precisare che la tecnologia in esame è anche utilizzata dall'INTERPOL: cfr., a riguardo, il presente link.

[3] Per un quadro di sintesi in merito all'utilizzo del riconoscimento facciale in alcuni Paesi europei (tra cui, in particolare, la Francia, la Germania e il Regno Unito) si veda il recente *report* dell'European Union Agency for Fundamental Rights (FRA), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, reperibile a questo link, pp. 11 ss. Una più ampia mappatura delle autorità di *law enforcement* UE che adoperano i meccanismi in questione è reperibile, consultando il seguente articolo: Kayser-Bril, *At least 10 police forces use face recognition in the EU, AlgorithmWatch reveals*, al presente link.

[4] Sulla tematica – che sarà approfondita *infra* § 5 – si veda, in particolare, l'ampia analisi di Lopez (2019), pp. 239 ss. e Valli (2019).

[5] Per una chiara spiegazione del funzionamento dei *tools* in esame, cfr. European Union Agency for Fundamental Rights (FRA), *Facial recognition technology,* cit., pp. 7 s. Cfr. anche Hern, *What is facial recognition – and how do police use it?*, in *www.theguardian.com*, 24 gennaio 2020.

[6] Così, efficacemente, Lopez (2019), p. 241.

[7] Si vedano, in proposito, IJIS Institute, *Law enforcement Facial Recognition Use Case Catalog*, al presente link; Information Technology & Innovation Foundation (ITIF), *The Value of Facial Recognition in Law Enforcement*, al presente link, nonché Castro e McLaughlin, *Banning Facial Recognition in Police Body Cameras Will Make Californians Less Safe*, al presente link, 10 settembre 2019. Per alcuni esempi concreti delle potenzialità dei mezzi in esame ai fini di contrasto della criminalità, cfr. McCarthy, *Facial recognition leads cops to alleged rapist in under 24 hours*, in *www.nypost.com*, 5 agosto 2019, nonché – con riguardo all'Italia – *Ladri individuati grazie al nuovo sistema di riconoscimento facciale*, in *www.ansa.it*.

[8] In realtà, gli strumenti in questione possono essere utilizzati anche per individuare soggetti vittime di reati, oppure, più generalmente, persone scomparse (in proposito, v. European Union Agency for Fundamental Rights (FRA), *Facial recognition technology,* cit., p. 25).

diretta i flussi video *live* provenienti dalle telecamere presenti in una zona[9]; di selezionare dai *frame* delle immagini le impronte facciali delle persone riprese e di cercare, infine, un *match* tra quest'ultime e i volti contenuti in un archivio di partenza.

Se ciò è vero, va peraltro precisato che numerosi studi hanno, da tempo[10], affermato che queste forme di IA sarebbero affette da significative criticità[11], le quali controbilancerebbero i vantaggi assicurati dalle stesse (sino – secondo molti – ad azzerarli). I *software* di riconoscimento facciale sono stati tacciati, per un verso, di risultare poco affidabili[12], potendo essere indotti a produrre risultati non attendibili dalla scarsa qualità delle immagini, dalla luce e da vari altri fattori[13], nonché, per un altro verso, di essere mezzi discriminatori[14]. A quest'ultimo riguardo, una recente, assai ampia ricerca del *National Institute of Standards and Technology*[15] degli Stati Uniti ha, ad esempio, dimostrato che la maggior parte degli algoritmi di *facial recognition* oggi in commercio manifesta dei *bias*; e ciò in quanto essi producono – tra l'altro – un numero di errori molto più alto nei confronti delle persone afro-americane (specie se donne) e asiatiche rispetto ai caucasici.

Non è però tutto. Va, infatti, rilevato come sia stata da molti denunciata la possibile frizione di tali tecnologie con plurimi altri diritti fondamentali dell'uomo, tra cui, *in primis*, i diritti alla *privacy* e alla protezione dei dati personali[16], essendovi persino il rischio che gli stessi siano utilizzati quali strumenti di sorveglianza di massa[17]. D'altra parte, il recente "scandalo *Cle-*

[9] La tecnologia è utilizzabile tanto per il tramite di telecamere fisse, quanto su dispositivi video portatili (si pensi, ad esempio, alle cd. *body cameras*, munite di riconoscimento facciale, in dotazione di diverse forze di polizia nordamericane. Sul punto, v. Murphy (2018), pp. 1 ss.; Ringrose (2019), pp. 57 ss.).

[10] Pare utile precisare che il tema del riconoscimento facciale non è nuovo, ma è dibattuto da vari decenni, specie nei sistemi di *common law*. Ad esempio, già sul finire degli anni Novanta e nei primi anni Duemila la dottrina statunitense ha iniziato ad analizzare in modo critico l'impatto di questo strumento sui diritti fondamentali dell'individuo. Si vedano, in proposito, tra i molti, Bennett (2002), pp. 151 ss.; Brogan (2002), pp. 65 ss.; Bowyer (2004), pp. 9 ss.; Fretty (2011), pp. 430 ss.; Gates (2006), pp. 417 ss.; Iraola (2003), pp. 773 ss.; McCoy (2002), pp. 471 ss.; Milligan (1999), pp. 295 ss.; Thornburg (2002), pp. 321 ss.; Woodward (1999), pp. 385 ss.; Id. (1997), pp. 97 ss. Per un quadro di sintesi del dibattito statunitense in tema di mezzi investigativi tecnologici, in grado di impattare sulla *privacy*, cfr. Di Paolo (2008), pp. 17, 26, 33 e 169 ss.

[11] In proposito, v. Big Brother Watch, *Face off. The lawless growth of facial recognition in UK policing*, al presente link; Carlo, *Facial recognition: what it is and why you should care*, in *www.libertyhumanrights.org.uk*, 23 agosto 2017; Facial Recognition Working Group of the Biometrics and Forensics Ethics Group, *Ethical issues arising from the police use of live facial recognition technology*, al presente link, Fussey e Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology,* Human Rights Centre, University of Essex, al presente link; London Policing Ethics Panel, *Final report on live facial recognition*, al presente link, pp. 42 ss.; Lynch, *Face Off: Law enforcement use of face recognition technology,* al presente link; Garvie e Moy, *America under watch*, cit. In lingua italiana, si veda l'analisi di Lopez (2019), pp. 244 ss.

[12] Al riguardo, v. Big Brother Watch, *Face off*, cit., p. 15.; Dodd, *UK police use of facial recognition technology a failure, says report*, in *www.theguardian.com*, 15 maggio 2018; Manthorpe e Martin, *81% of 'suspects' flagged by Met's police facial recognition technology innocent, independent report says*, in *www.news.sky.com*, 4 luglio 2019; Sharman, *Metropolitan Police's facial recognition technology 98% inaccurate, figures show*, in *www.independent.co.uk*, 13 maggio 2018.

[13] Per alcuni esempi, cfr. Sacchetto (2019), p. 471. Ai limiti tecnici del sistema, si aggiungono poi gli abusi che mediante lo stesso possono essere scientemente perpetuati: si veda, in proposito, il recente studio di Garvie, *Garbage in, Garbage Out. Face Recognition on Flawed Data*, al presente link, laddove si è denunciato l'utilizzo da parte di alcune forze di polizia degli USA, in mancanza di foto chiare e definite di sospettati, di immagini di personaggi (famosi), considerati somiglianti ai ricercati.

[14] Cfr., in proposito, tra i molti, Buolamwini, *Response; Racial and Gender bias in Amazon Rekognition – Commercial AI System for Analyzing Faces*, in *www.medium.com*, 25 gennaio 2019; Ead., *When the Robot Doesn't See Dark Skin*, in *www.nytimes.com*, 21 giugno 2018; Buolamwini e Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, al presente link; Concerned Researchers, *On Recent Research Auditing Commercial Facial Analysis Technology*, in *www.medium.com*, 26 marzo 2019; Garvie e Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, in *www.theatlantic.com*, 7 aprile 2016; Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias*, in *www.nytimes.com*, 8 luglio 2019; Hoggins, *'Racist and sexist' facial recognition cameras could lead to false arrests*, in *www.telegraph.co.uk*; Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, in *www.nytimes.com*, 9 febbraio 2018; Porter, *Federal study of top facial recognition algorithms finds "empirical evidence" of bias*, in *www.theverge.com*, 20 dicembre 2019; Morrison, *"Racist" facial recognition technology used in law enforcement, banking and schools misidentifies African American and Asian people 100 times more often than whites, study shows*, in *www.dailymail.co.uk*, 19 dicembre 2019. Pare utile ricordare che, preso atto di tale criticità, l'European Data Protection Board, nelle sue *Guidelines 3/2019 on processing of personal data through video devices*, adottate il 10 luglio 2019, ha affermato che «*bias in facial recognition threatens to reinforce the prejudices of society. That is why, data controllers must also ensure that biometric data processing deriving from video surveillance be subject to regular assessment of its relevance and sufficiency of guarantees provided*».

[15] Ci si riferisce nello specifico al recente studio di Grother, Ngan, Hanaoka, *Face Recognition Vendor Test (FVRT). Part 3: Demographic Effects,* reperibile al presente link, p. 2 e s. Per una presentazione di tale studio, cfr. *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, in *www.nist.gov*, 19 dicembre 2019, nonché Singer e Metz, *Many Facial-Recognition Systems Are Biased, Says U.S. Study*, in *www.nytimes.com*, 19 dicembre 2019.

[16] In proposito, v., ad esempio, European Union Agency for Fundamental Rights (FRA), *Facial recognition technology,* cit., pp. 23 ss.; Wiewiórowski, *Facial recognition: A solution in search of a problem?,* al presente link, nonché il Libro bianco del 19 febbraio 2020 della Commissione europea, *sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, COM (2020) 65 final, p. 24.

[17] Al riguardo, cfr. Chandran, *Mass surveillance fears as India readies facial recognition system*, in *www.reuters.com*, 7 novembre 2019; Garvie e Moy, *America under watch*, cit. Lo scorso anno ha fatto, ad esempio, assai scalpore l'utilizzo da parte della polizia cinese della tecnologia in esame per individuare e controllare la minoranza musulmana degli Uiguri: in proposito, cfr. Mozur, *One Month, 500.000 Face Scans: How China Is Using A.I. to Profile a Minority*, in *www.nytimes.com*, 14 aprile 2019.

arview", scoppiato negli Stati Uniti a seguito di un'inchiesta del *New York Times*[18], dimostra come, anche nelle democrazie occidentali, sia tutt'altro che infondato il timore circa il fatto che gli strumenti di riconoscimento facciale si possano trasformare in mezzi in grado di contribuire a un "clima orwelliano" di intrusione ossessiva nella sfera di riservatezza dei singoli.

Tenuto conto dell'esistenza di un contesto di fondo tanto problematico, non stupisce che la schiera di coloro che criticano la possibilità per le autorità di *law enforcement* di avvalersi di strumenti di riconoscimento facciale, senza che siano messe in campo adeguate salvaguardie, abbia, negli ultimi tempi, incrementato oltremodo i propri sforzi per migliorare lo *status quo*[19]. Va, peraltro, notato che le frange più estreme di tale movimento non hanno, invero, solo proposto a più riprese di introdurre a livello normativo delle moratorie generali nei confronti di siffatti strumenti[20], ma sono riuscite effettivamente anche già a ottenere – quantomeno negli USA – il divieto per le forze di polizia di alcune città[21] e Stati[22] di continuare a utilizzare questi mezzi tecnologici.

Ciò premesso, è d'uopo precisare che – ad oggi – la grande assente del dibattito globale in tema di *facial recognition* è senza alcun dubbio la giurisprudenza. Come ha riconosciuto l'Agenzia dell'Unione Europea per i diritti fondamentali, sono, infatti, finora stati quantomai rari i casi in cui delle Corti si siano pronunciate sulla legittimità della tecnologia *de qua*[23]. Ed è proprio alla luce di siffatta radicale carenza di decisioni giudiziali in materia (tanto in Italia, quanto all'estero) che emerge l'importanza chiave della sentenza qui pubblicata dell'*High Court of Justice* dell'Inghilterra e Galles[24]. Essa è stata, infatti, a più voci definita come il primo arresto a livello mondiale[25] ad aver affrontato in modo analitico la questione della compatibilità dell'utilizzo da parte della polizia di mezzi di riconoscimento facciale con i diritti fondamentali alla riservatezza e alla tutela dei dati personali.

[18] Ci si riferisce, più precisamente, al fatto che, secondo quanto riportato da tale noto quotidiano (Hill, *The Secretive Company That Might End Privacy as We Know It*, in *www.nytimes.com*, 18 gennaio 2020), la società *Clearview* avrebbe dato vita a un'immensa banca dati di miliardi di immagini (estrapolate illegalmente da Facebook, Twitter, Youtube, Venmo e molti altri siti internet), la quale sarebbe servita da *database* per il funzionamento di un *tool* di *facial recognition*, venduto a un gran numero di forze di polizia nordamericane e canadesi, che lo avrebbero poi utilizzato senza porsi problemi circa la provenienza della mole immensa di dati sensibili via via processati. Com'era prevedibile, l'emersione dello scandalo *de quo* non ha solo indotto grandi aziende come Twitter a diffidare la società in questione a continuare a utilizzare le sue immagini (Hill, *Twitter Tells Facial Recognition Trailblazer to Stop Using Site's Photos*, in *www.nytimes.com*, 22 gennaio 2020), oppure il Procuratore generale del New Jersey a vietare alla polizia di avvalersi tale *software* (Hill, *New Jersey Bars Police From Using Clearview Facial Recognition App*, in *www.nytimes.com*, 24 gennaio 2020), ma ha, più in generale, contribuito a rendere (tanto all'interno, quanto all'esterno degli Stati Uniti) ancora più acceso lo scontro tra sostenitori e detrattori dei mezzi di *facial recognition*.

[19] Ad esempio, negli Stati Uniti è stata di recente presentata una proposta *bipartisan* di legge federale (ci si riferisce al *Facial Recognition Technology Warrant Act of 2019*, S. 2878, reperibile al seguente link), attualmente in discussione al Congresso, volta a stabilire alcune significative tutele processuali con riguardo all'utilizzo da parte delle forze di polizia federali degli algoritmi di riconoscimento facciale. L'atto *de quo* si propone, in estrema sintesi, di imporre alle autorità di *law enforcement*, per poter avvalersi dei *tools* in esame ai fini di sorveglianza fisica sugli individui, di ottenere (di norma) un previo mandato giudiziale, che autorizzi l'attività captativa. Pare utile precisare che non si tratta affatto della prima proposta in materia. Nel corso degli anni, si sono infatti susseguite, specie a livello statale, diverse iniziative volte a limitare l'utilizzo dei *tools* in esame: sul punto, cfr. Hrick e F. Heydari, *The Growing World of Face Recognition Legislation: A Guide to Enacted and Proposed Legislation*, reperibile al presente link.

[20] A tal proposito, va ricordato che, dopo lo scandalo *Clearview*, 40 organizzazioni a tutela della *privacy* hanno inviato una lettera al Presidente degli Stati Uniti, onde ottenere una moratoria generalizzata sull'utilizzo del riconoscimento facciale ai fini di *law enforcement*: in proposito, v. Tech Policy, *40 groups have called for a US moratorium on facial recognition technology*, in *Mit Technology Review*, 27 gennaio 2020. Per alcune acute considerazioni critiche su tale approccio massimalista: cfr. Schneier, *We're Banning Facial Recognition. We're Missing the Point*, in *www.nytimes.com*, 20 gennaio 2020.

[21] Ad esempio, nel 2019 San Francisco, Somerville e Oakland hanno vietato l'utilizzo da parte delle forze di polizia della tecnologia *de qua*: cfr., in proposito, il presente link.

[22] Un divieto temporaneo è, ad esempio, stato adottato nel 2019 nello Stato della California: sul punto v. *California Governor Signs Landmark Bill Halting Facial Recognition on Police Body Cams*, in *www.aclunc.org*, nonché Metz, *California lawmakers ban facial-recognition software from police body cams*, in *www.edition.cnn.com*, 13 settembre 2019.

[23] In proposito, v. European Union Agency for Fundamental Rights (FRA), *Facial recognition technology,* cit., p. 4, ove si afferma che, in questa materia, «*case law is still virtually non-existent*».

[24] Cfr. High Court of Justice, Queen's Bench Division, Divisional Court, 4 settembre 2019, Case No: CO/4085/2018, R (Bridges) v. CCSWP e SSHD (d'ora in avanti la pronuncia sarà così abbreviata: [2019] EWHC 2341 (Admin)). Per un commento alla decisione (di primo grado) in esame, cfr. Dobson, *Use of automatic facial recognition software*, in *The Law Society Gazette*, 14 ottobre 2019; Kotsoglou e Oswald (2020), pp. 86 ss.; Inside Privacy, *UK Court upholds police use of automated facial recognition technology*, in *www.insideprivacy.com*, 16 settembre 2019; Maini-Thompson, *Facial Recognition Technology: High Court gives judgment*, in *www.ukhumanrightsblog.com*, 12 settembre 2019. Una chiara spiegazione in merito al funzionamento e alla competenza della *High Court of Justice* si può trovare in Gillespie e Weare (2019), pp. 212 ss. In lingua italiana, cfr., per tutti, Mattei (2010), pp. 68 ss.

[25] In questo senso, cfr., ad esempio, Liberty, *Liberty fights for facial recognition ban following Court ruling*, al presente link, nonché Dearden, *Police used facial recognition technology lawfully, High Court rules in landmark challenge*, in *www.independent.co.uk*, 4 settembre 2019. Si veda anche [2019] EWHC 2341 (Admin), § 1.

2. Il progetto pilota della *South Wales Police* in tema di riconoscimento facciale.

Per comprendere appieno la pronuncia in esame è, peraltro, indispensabile ricostruire in via preliminare il contesto in cui la stessa è maturata.

A tal proposito, è bene ricordare che nel Regno Unito diversi corpi di polizia stanno negli ultimi anni sperimentando l'utilizzo del riconoscimento facciale, ai fini di prevenzione e repressione della criminalità, tramite una serie di progetti pilota[26], i quali sono stati avviati pur in assenza di alcuna disciplina legislativa specifica che regoli tale assai delicata attività[27].

Il ruolo di *leader* in quest'ambito è stato assunto dalla *South Wales Police*[28], la quale, grazie anche ad alcuni finanziamenti governativi, ha iniziato, sin dagli inizi del 2017, un progetto concernente la tecnologia in esame, in vista di una sua possibile diffusione a livello nazionale[29].

Il programma così avviato (tutt'ora in corso) contempla l'utilizzo dei *software* di riconoscimento in due modi diversi. Il primo è noto come "*AFR Identify*" e consiste nell'analisi statica, attraverso un algoritmo di *facial recognition*, di un'immagine di un soggetto la cui identità è ignota, la quale viene comparata con quelle contenute in un *database* della *South Wales Police* (contenente un bacino di circa cinquecentomila profili facciali)[30]. Il secondo è, invece, denominato "*AFR Locate*": esso prevede la ripresa *live* tramite telecamere posizionate sul territorio dei volti di soggetti che si trovino in determinati luoghi di interesse, finalizzata all'estrazione del profilo facciale di tali individui[31]; siffatte informazioni sono poi confrontate, tramite un *software*, con i modelli biometrici di persone inserite in una lista *ad hoc* più ristretta (la cui capacità massima è di duemila immagini), preparata dalla *South Wales Police* per il singolo evento di interesse[32] (cd. *watchlist*).

A questo punto, laddove il *software* identifichi un possibile *match* tra profili biometrici «*the two images are reviewed by an AFR operator ("the system operator", who is a police officer) to establish whether he believes that a match has in fact been made*»[33]. Com'è ovvio, il fatto che un operatore in carne ed ossa debba sempre intervenire (pur nella fase finale dell'attività del *tool*) rappresenta una salvaguardia di importanza fondamentale per i diritti dei singoli: l'intervento umano è, infatti, una garanzia importante, in grado di ridurre (ma non di eliminare)[34] la probabilità che un soggetto sia ingiustamente arrestato a causa di un errore dell'algoritmo[35].

Da un punto di vista pratico, l'attività di sperimentazione dei *software* di riconoscimento facciale è stata portata avanti in modo massiccio. La polizia gallese ha, ad esempio, utilizzato il sistema "*AFR Locate*" in più di cinquanta occasioni tra maggio 2017 e l'aprile 2019 in una larga varietà di pubblici eventi[36], tra cui la finale di UEFA *Champions League* di Cardiff del 2017, in occasione della quale è stato compiuto il primo arresto in diretta tramite mezzi di riconoscimento facciale[37]. Non si pensi, peraltro, che siffatto progetto pilota sia stato svolto senza alcuna difficoltà: è d'uopo, infatti, precisare come sia stato a più voci denunciato il fatto che l'algoritmo utilizzato dalla polizia gallese fosse – specie in un primo momento – affetto da

[26] Ci si riferisce alla *London Metropolitan Police*, alla *South Wales Police* e alla *Leicestershire Police*: in proposito, v. The Law Society of England and Wales, *Algorithms in the Criminal Justice System*, 2019, reperibile al seguente link, p. 37 s., nonché l'ampio studio di Purshouse e Campbell (2019), pp. 188 ss.

[27] In proposito, v. Big Brother Watch, *Face off*, cit., p. 9; Purshouse e Campbell (2019), p. 198; Fussey e D. Murray, *Independent Report on the London Metropolitan Police Service's*, cit., p. 49; The Law Society of England and Wales, *Algorithms in the Criminal Justice System*, cit., p. 41.

[28] Così, Purshouse e Campbell (2019), p. 190.

[29] Una grande mole di informazioni, concernenti l'utilizzo da parte della polizia gallese della tecnologia in esame, si può trovare al seguente link. È interessante notare come la *South Wales Police* pubblichi sul suo sito *web* l'intero elenco degli eventi e delle operazioni in cui le attività captative sono state compiute, nonché la quantità di *alerts* forniti dal sistema in ogni singola occasione e di arresti effettuati mediante l'utilizzo della tecnologia *de qua*.

[30] Cfr. [2019] EWHC 2341 (Admin), § 27.

[31] Ancora [2019] EWHC 2341 (Admin), §§ 28 ss.

[32] [2019] EWHC 2341 (Admin), § 31.

[33] Così, testualmente, [2019] EWHC 2341 (Admin), § 33.

[34] In proposito, v. Lopez (2019), p. 244.

[35] Anche la pronuncia in esame ha affermato che «*the fact that human eye is used to ensure that an intervention is justified, is an important safeguard*» ([2019] EWHC 2341 (Admin), § 33).

[36] Cfr. [2019] EWHC 2341 (Admin), § 28.

[37] A riguardo, v. il seguente articolo: Bridge, *Police make first arrest using facial recognition surveillance cameras at Cardiff Millennium stadium*, in *www.thetimes.co.uk*, 8 giugno 2017.

un tasso di errore particolarmente elevato[38]. A riprova di ciò, basti pensare che, nel corso della citata finale di *Champions League* del 2017, oltre duemila persone sono state erroneamente identificate quali possibili criminali dal *tools*[39]. Peraltro, come confermato da una ricerca compiuta dall'Università di Cardiff sull'utilizzo da parte della polizia dei *software* in questione[40], «*over the period of the evaluation the accuracy of the technology improved significantly and police got better at using it*»[41]. Un tanto testimonia come la tecnologia *de qua* si trovi ancora in una fase di intenso rodaggio, necessitando di continui affinamenti per risultare affidabile e per limitare il rischio che la stessa sia affetta da *bias* cognitivi.

3. La decisione della *High Court*.

La pronuncia in commento ha alla base proprio l'utilizzo da parte della *South Wales Police* del sistema "*AFR Locate*" nei confronti di un attivista per i diritti civili, tale Edward Bridges. Più precisamente, quest'ultimo, avvalendosi dell'ausilio della nota associazione per la protezione dei diritti umani *Liberty*[42], ha adito la *High Court of Justice* onde censurare di essere stato illegalmente sottoposto al sistema *AFR Locate*, senza il suo consenso e senza essere preavvertito di ciò, in due diverse occasioni, mentre si trovava a Cardiff[43]. A tale riguardo, va ricordato che egli non faceva parte dei soggetti inseriti nelle liste di sospettati (cd. *watchlist*), stilate dalla polizia gallese, essendo soltanto un comune cittadino che si trovava nei luoghi sottoposti a video sorveglianza[44].

Gli argomenti che Bridges ha addotto a sostegno del suo ricorso sono – in estrema sintesi – tre. A suo dire, la *South Wales Police*, sottoponendo all'algoritmo di riconoscimento facciale, in assenza di una disciplina legislativa *ad hoc* che autorizzasse tale attività, avrebbe: a) leso il suo diritto alla riservatezza, tutelato dall'art. 8 CEDU[45]; b) violato la disciplina eurounitaria[46] e interna[47] di protezione dei dati personali[48]; c) trasgredito l'*Equality ACT* del 2010[49] (ossia un provvedimento, volto a proteggere le persone contro ingiuste discriminazioni), essendovi il concreto rischio che il *software* di *facial recognition* fosse affetto da *bias* cognitivi nei confronti delle donne e di minoranze etniche[50].

È, pertanto, evidente come il ricorso di Bridges sia stato stilato ad arte, in modo tale da sintetizzare l'insieme delle critiche più rilevanti, sollevate da plurimi studiosi e associazioni a tutela dei diritti umani nei confronti dell'utilizzo da parte delle autorità di *law enforcement* dei mezzi tecnologici in questione. L'obiettivo del ricorrente (e di *Liberty*) era, in sostanza, quello di ottenere una pronuncia giudiziale, che confermasse l'esistenza di tali problematiche di fondo dei *software* di *facial recognition*.

Dal canto suo, la *High Court of Justice* ha però disatteso simili aspettative: essa ha, infatti, rigettato tutte le menzionate censure, mediante una motivazione alquanto articolata, così riassumibile.

[38] Sul punto, v. Purshouse e Campbell (2019), p. 191.
[39] In proposito, v. il presente articolo della BBC: *2,000 wrongly matched with possible criminals at Champions League*, in *www.bbc.com*, 4 maggio 2018.
[40] Ci si riferisce al report di Davies, Innes, Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, reperibile al presente link.
[41] La citazione è tratta dal seguente *post*: *Evaluating the Use of Automated Facial Recognition Technology in Major Policing Operations*, reperibile al presente link. Il *post* continua affermando che, secondo l'analisi dell'Università di Cardiff, «*the Locate system was able to correctly identify a person of interest around 76% of the time. A total of 18 arrests were made in 'live Locate deployments during the evaluation, and in excess of 100 people were charged following investigative searches during the first 8-9 months of the AFR Identify operation*».
[42] Si veda, per maggiori informazioni, il sito dell'organizzazione reperibile a questo link.
[43] [2019] EWHC 2341 (Admin), §§ 11 ss.
[44] In proposito, v. [2019] EWHC 2341 (Admin), § 16.
[45] Si veda [2019] EWHC 2341 (Admin), § 19.
[46] Il riferimento va in particolare alla direttiva 2016/680/UE, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, in *G.U.U.E.*, 4 maggio 2016, L 119/89. Per un recente commento al provvedimento *de quo*, cfr. l'ampia analisi di González Cano (2019), pp. 1331 ss.
[47] Le censure riguardavano, in particolare, la violazione del *Data Protection Act* del 1998 e del *Data Protection Act* del 2018. Per una guida alla disciplina britannica in tema di protezione dei dati personali, si consulti il seguente link.
[48] Cfr. [2019] EWHC 2341 (Admin), § 20.
[49] In proposito, v. il seguente link.
[50] V. [2019] EWHC 2341 (Admin), § 20.

Con riguardo al primo motivo di ricorso, la Corte ha ammesso che l'utilizzo da parte della polizia gallese del *software* di *facial recognition* ha determinato un'ingerenza nella vita privata di Bridges, potenzialmente lesiva dell'art. 8 CEDU[51]; e ciò in quanto l'algoritmo di riconoscimento, avendo estratto il suo profilo facciale, avrebbe permesso di acquisire «*information of an "intrinsically private" character*»[52]. Una siffatta invasione nella sua sfera di riservatezza è stata però considerata del tutto legittima, poiché consentita dall'art. 8, par. 2, CEDU[53], il quale – com'è noto – prevede che le autorità pubbliche possano compiere un'intrusione nella *privacy* dei singoli, laddove siffatto comportamento sia previsto «dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

A tal proposito, la pronuncia in esame ha ritenuto non condivisibile la tesi del ricorrente – secondo cui le autorità di *law enforcement* non avrebbero in ogni caso rispettato la riserva di legge di cui all'art. 8, par 2, CEDU, in ragione della mancanza di una disciplina legislativa *ad hoc* in tema di riconoscimento facciale[54] – facendo leva in particolare su due argomenti. In primo luogo, una siffatta tesi non è stata condivisa dai giudicanti, dal momento che essi hanno ritenuto che l'attività di raccolta e di conservazione di dati biometrici facciali tramite algoritmi debba essere fatta rientrare tra i poteri generali che il *common law* attribuisce alle forze di polizia per prevenire e contrastare la criminalità[55]. Per di più – ed in secondo luogo – la Corte ha negato che il sistema giuridico d'oltremanica sia realmente sprovvisto del tutto di una disciplina normativa in tema di *facial recognition*[56], dal momento che tali strumenti rientrano comunque nell'ambito di applicazione delle previsioni comuni (interne ed eurounitarie) di tutela della *privacy*[57], a cui vanno aggiunte una serie di disposizioni di rango regolamentare in tema di video sorveglianza[58] e di *local policies*, adottate dalla *South Wales Police*[59]. In definitiva, a detta della *High Court*, il combinato disposto tra il *common law*, la *primary legislation* (generale) in materia di *privacy* e una serie di norme di rango non legislativo andrebbe a costituire quel «*clear and sufficient legal framework governing whether, when and how AFR Locate may be used*»[60], idoneo a soddisfare lo *standard* di cui all'art. 8, par. 2, CEDU.

È d'uopo, peraltro, ricordare che, prima di arrivare a una siffatta conclusione, i decisori hanno considerato opportuno distinguere il riconoscimento facciale, da una parte, e l'estrazione di un profilo del DNA/il rilievo delle impronte digitali, da un'altra parte[61]. A detta dei giudici d'oltremanica, infatti, tra tali strumenti tecnici sussisterebbe una differenza di primario rilievo: mentre il DNA e la raccolta delle impronte digitali «*involve physically intrusive acts*»[62], al contrario «*no physical entry, contact or force is necessary when using AFR Locate to obtain biometric data*»[63]. Ed è proprio la constatazione per cui la scansione tramite algoritmi di *facial recognition* non andrebbe a determinare un'ingerenza fisica diretta sulle persone ha portato la Corte ad affermare che, allo stesso modo di quanto accade per le videoriprese[64] (e a differenza di quanto avviene per mezzi considerati più intrusivi come proprio il DNA e la raccolta delle

[51] Sul punto, v. [2019] EWHC 2341 (Admin), § 62. In questo contesto, la *High Court* ha richiamato a più riprese la pronuncia Corte edu, Grande Camera, 4 dicembre 2008, *S. e Marper c. Regno Unito*, la quale al § 67 ha affermato che «*the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8*». Nello stesso senso, si veda, più di recente, Corte edu, sez. V, 30 gennaio 2020, *Breyer c. Germania*, § 81.
[52] Così, testualmente, [2019] EWHC 2341 (Admin), § 57.
[53] [2019] EWHC 2341 (Admin), § 96.
[54] In proposito, v. [2019] EWHC 2341 (Admin), §§ 63 e s.
[55] Sul punto, si veda in particolare [2019] EWHC 2341 (Admin), § 78.
[56] Al riguardo, v. [2019] EWHC 2341 (Admin), § 84.
[57] Cfr. [2019] EWHC 2341 (Admin), § 85. In sostanza, sebbene il *Data Protection Act* del 2018 non contempli norme *ad hoc* in tema di riconoscimento facciale, i giudici britannici hanno messo in rilievo come siffatta fonte detti però una serie di previsioni applicabili a ogni forma di trattamento di dati sensibili da parte delle autorità di polizia, le quali vanno rispettate anche in caso siano utilizzati gli algoritmi in esame.
[58] Il rinvio va, in particolare, al *Surveillance Camera Code of Practice*, il quale rappresenta un provvedimento «*issued by the Home Secretary pursuant to section 30 of the Protection of Freedoms Act 2012 ("the 2012 Act"); it contains guidance about the use of surveillance camera systems*» (così [2019] EWHC 2341 (Admin), § 89).
[59] In proposito, v. [2019] EWHC 2341 (Admin), §§ 92 ss.
[60] Cfr. [2019] EWHC 2341 (Admin), § 84.
[61] A questo riguardo, v. [2019] EWHC 2341 (Admin), §§ 73 ss.
[62] Così, [2019] EWHC 2341 (Admin), § 75.
[63] La citazione è tratta ancora da [2019] EWHC 2341 (Admin), § 75.
[64] Si veda, a riguardo, in particolare [2019] EWHC 2341 (Admin), §§ 73 e 75, ove i giudici hanno statuito che il metodo del riconoscimento facciale «*is no more intrusive than the use of CCTV in the streets*».

impronte[65]), non sarebbe affatto necessario che le autorità di *law enforcement* siano dotate di «*new express statutory powers*»[66] per poter legittimamente avvalersi dei *software* di analisi biometrica in esame.

Come anticipato, neppure la seconda macro-censura sollevata da Bridges, concernente la violazione della disciplina generale in materia di tutela della *privacy*, ha avuto migliore fortuna. Difatti, a detta della Corte d'oltremanica, non solo la procedura di profilazione a cui è stato sottoposto il ricorrente, nel momento in cui il suo volto è stato scansionato dal *software* di riconoscimento, è stata compiuta al fine di perseguire lo scopo del tutto legittimo di prevenire e contrastare la criminalità, ma la *South Wales Police* avrebbe anche rispettato tutti i requisiti specifici, stabiliti dalla legge (interna ed eurounitaria), per i casi in cui siano trattate categorie particolari/sensibili di dati personali[67] (*genus* all'interno del quale sono stati fatti rientrare i dati biometrici, tesi a identificare in modo univoco una persona fisica, quali quelli ottenuti tramite la tecnologia di *facial recognition*). Ad esempio, va a tal proposito ricordato che la *South Wales Police*, oltre ad aver messo in campo uno *standard* di garanzie particolarmente elevato in tema di *data retention*[68], ha anche adottato specifici accorgimenti «*to inform members of the public about AFR and as to its use at the event or in the area which they may be attending or present*»[69]. A ogni modo, a convincere i giudici circa la necessità di rigettare le censure in tema di *privacy*, è stato, in particolare, il fatto che la polizia gallese, prima di compiere l'attività di videoripresa mediante *facial recognition*, avesse adottato, per un verso, un documento programmatico, intitolato "*Policy on Sensitive Processing for Law Enforcement Purposes*"[70], con cui ha spiegato le procedure messe in campo «*for securing compliance with the data protection principles*»[71] e, per un altro verso, un *Data Protection Impact Assessment*[72], volto a chiarire il funzionamento del sistema "*AFR Locate*" e i rischi per la protezione dei dati personali determinati dallo stesso (nonché le contromisure messe in campo per contrastare siffatti pericoli).

Infine, il terzo motivo di ricorso, con cui Bridges si è lamentato dei possibili effetti discriminatori dell'algoritmo di riconoscimento nei confronti delle donne e di minoranze etniche, non ha trovato accoglimento, perché considerato privo di un sufficiente apporto probatorio. Sebbene, infatti, la difesa si sia avvalsa a questo proposito di un consulente, il quale ha – tra l'altro – sostenuto che «*bias has been found to be a feature of common AFR systems*»[73], la *High Court* ha, dal canto suo, ritenuto che, nel caso di specie, non vi fosse «*firm evidence that the software does produce results that suggest indirect discrimination*»[74]. Per giungere a una tal conclusione, i giudici hanno valorizzato in particolare la circostanza per cui la *South Wales Police* avesse adottato – pur se soltanto nelle fasi iniziali della sperimentazione della tecnologia in esame – un documento, intitolato "*Equality Impact Assessment - Initial Assessment*"[75], con cui aveva soppesato i rischi di effetti discriminatori derivanti dall'applicazione della tecnologia *de qua*. Ebbene, la presenza di tale provvedimento, sommata al fatto che, in una fase successiva del progetto pilota, un ufficiale della *South Wales Police* avesse diffuso informazioni sul tasso di errori verificatisi nell'utilizzo dell'algoritmo, affermando di aver «*reviewed the use of AFR Locate for bias based on ethnic origin*»[76] (e di non aver trovato concreta evidenza di un tale problema), hanno portato la Corte a ritenere che la polizia gallese abbia rispettato anche da questo profilo i diritti dell'uomo.

[65] In proposito, cfr. [2019] EWHC 2341 (Admin), § 73, laddove la Corte ha statuito che «*specific statutory powers were needed for e.g. the taking of fingerprints, and DNA swabs to obviate what would otherwise be an assault*».
[66] [2019] EWHC 2341 (Admin), § 78.
[67] In proposito, v., in particolare, [2019] EWHC 2341 (Admin), §§ 122 ss.; 133 e s.; 139 s. 144 ss.
[68] Al riguardo, v. [2019] EWHC 2341 (Admin), § 37 e s., ove si ricorda, ad esempio, che nel sistema *AFR Locate*, se un profilo facciale non determina alcun *match* con quelli contenuti nella base di dati di riferimento, viene immediatamente eliminato.
[69] La citazione è tratta da [2019] EWHC 2341 (Admin), § 39. Ci si riferisce, più precisamente, al fatto che la polizia gallese non solo dia avviso tramite *social network* dell'inizio delle operazioni captative, ma anche alla circostanza per cui essa utilizzi nel corso delle attività veicoli speciali, facilmente riconoscibili dal pubblico, sui quali si fa visivamente riferimento alla loro funzione di mezzi dedicati al riconoscimento facciale.
[70] Cfr. [2019] EWHC 2341 (Admin), § 139.
[71] La citazione è tratta da [2019] EWHC 2341 (Admin), § 138.
[72] V. [2019] EWHC 2341 (Admin), §§ 147 s.
[73] Così, testualmente, [2019] EWHC 2341 (Admin), § 155.
[74] In proposito, v. [2019] EWHC 2341 (Admin), § 153.
[75] Si veda in particolare [2019] EWHC 2341 (Admin), § 158.
[76] Cfr. [2019] EWHC 2341 (Admin), § 154.

4. Le reazioni critiche alla pronuncia della Corte.

Com'era prevedibile, la decisione in commento – lungi dall'essere riuscita a dirimere il contrasto tra sostenitori e oppositori del riconoscimento facciale – è andata incontro ad accese critiche, sollevate da una pluralità di soggetti[77].

Il malcontento nei confronti dell'impostazione adottata dalla sentenza *Bridges* è stato, ad esempio, incanalato in una richiesta generale di moratoria sull'utilizzo del *facial recognition* ai fini di prevenzione e repressione dei reati, la quale è stata siglata non solo da un folto gruppo di enti deputati alla tutela dei diritti umani, ma anche da noti parlamentari del Regno Unito e da membri della società civile (avvocati e accademici)[78]. Questo eterogeneo gruppo di *stakeholders*, pur ammettendo di avere visioni anche piuttosto diverse circa il modo in cui disciplinare i mezzi tecnici in questione, hanno affermato di trovarsi tutti d'accordo sulla necessità «*to immediately stop using live facial recognition for public surveillance*»[79].

Merita, peraltro, rilevare che la pronuncia in esame ha suscitato plurime obiezioni anche da parte di diverse autorità garanti d'oltremanica[80], tra cui va menzionato soprattutto l'*Information Commissioner's Office* (d'ora in avanti *ICO*), ossia il garante per la *privacy UK*. Dal canto suo, l'*ICO* ha, infatti, pubblicato vari documenti, in cui ha messo in luce l'esistenza di importanti criticità in merito all'attuale uso della tecnologia di *live facial recognition* da parte delle forze di polizia in luoghi pubblici nel Regno Unito[81].

A tal proposito, il *Commissioner* ha affermato che, per garantire i diritti umani, è necessario compiere un assai meticoloso vaglio di proporzionalità sulla «*strict necessity*» di utilizzare gli strumenti in esame[82]. A detta del garante del Regno Unito, infatti, da un lato, il riconoscimento facciale dovrebbe essere impiegato solo per contrastare «*specific serious or violent crimes*»[83] e non per perseguire forme di reato bagatellari[84], mentre, da un altro lato, sarebbe sempre necessario spiegare il perché non possono essere utilizzati mezzi investigativi meno invasivi rispetto a quello tecnico *de quo*[85]. A tal proposito, l'*ICO* ha, più precisamente, statuito che il *facial recognition «may be likelier to meet the requirements of strict necessity and proportionality where it is deployed on a targeted or smaller-scale basis and for a narrowly defined purpose»*[86], il che avviene, ad esempio, laddove esso venga attivato in un luogo ben definito (come gli aeroporti), oppure quando vi sono già indizi circa la probabilità che un individuo sospettato di un (grave) reato possa trovarsi a una certa ora in un determinato luogo. Ciò posto, il garante ha colto l'occasione per criticare espressamente la pronuncia *Bridges*, affermando che, a suo parere, la polizia gallese in tale fattispecie non aveva rispettato lo stretto vaglio di necessità e proporzionalità in concreto imposto dalla tutela del diritto alla *privacy*[87]; e ciò in quanto la *South Wales Police* non

[77] Per un quadro di sintesi sul punto, cfr. Chertoff, *Facial Recognition Has Its Eye on the U.K.*, in *www.lawfareblog.com*, 7 febbraio 2020.

[78] Ci si riferisce alla lettera, redatta dall'organizzazione *Big Brother Watch*, nel settembre 2019, *Joint statement on police and private company use of facial recognition surveillance in the UK*, la quale è pubblicata al seguente link. In proposito, cfr. *Ban facial recognition cameras, MPs urge*, in *www.thetimes.co.uk*, 19 settembre 2019; Quach, *MPs call for 'immediate' stop to facial recog in UK as report underlines bias risks in 'pre-crime' algos used by coppers*, in *www.theregister.co.uk*, 18 settembre 2019.

[79] In questo senso si esprime testualmente la citata lettera *Joint statement on police and private company use of facial recognition surveillance in the UK.*

[80] Si veda, ad esempio, la riposta critica del *Commissioner for the Retention and Use of Biometric Material* (ossia l'autorità indipendente, funzionalmente deputata a controllare l'uso e la conservazione da parte delle forze di polizia britanniche di dati biometrici) alla sentenza *Bridges*, pubblicata con il titolo di *Automated facial recognition. Biometrics Commissioner response to court judgment on South Wales Police's use of automated facial recognition technology*, reperibile al seguente link.

[81] Ci si riferisce, in particolare, oltre all'articolo Denham (Information Commissioner), *Blog: Live facial recognition technology – police forces need to slow down and justify its use*, reperibile al link, ai seguenti *report*: Information Commissioner's Office, *ICO investigation into how the police use facial recognition technology in public places*, consultabile al link e Information Commissioner's Opinion, *The use of live facial recognition technology by law enforcement in public places*, reperibile al link. In proposito, v. Jungyun Choi, *AI/IoT Update: UK's Information Commissioner Issues Opinion on Use of Live Facial Recognition Technology by Police Forces*, in *www.insideprivacy.com*, 5 novembre 2019.

[82] Al riguardo, v. Information Commissioner's Opinion, *The use of live facial recognition technology by law enforcement in public places*, cit., p. 14 s.

[83] Sul punto, v. Information Commissioner's Opinion, *The use of live facial recognition technology by law enforcement in public places*, cit., p. 15. In termini analoghi, cfr. anche European Union Agency for Fundamental Rights (FRA), *Facial recognition technology,* cit., p. 34.

[84] Cfr., sul punto, Information Commissioner's Opinion, *The use of live facial recognition technology by law enforcement in public places*, cit., p. 17, ove il garante ha affermato che «*the inclusion of an image on a watchlist should meet the same high threshold for processing, ie, strict necessity. Watchlists comprising biometric images of individuals wanted or suspected of non-serious offences are, in the Commissioner's view, less likely to be able to satisfy that threshold*».

[85] Sul punto, v. Information Commissioner's Opinion, *The use of live facial recognition technology by law enforcement in public places*, cit., p. 15.

[86] Così, testualmente, Information Commissioner's Opinion, *The use of live facial recognition technology by law enforcement in public places*, cit., p. 15.

[87] Sul punto, si veda ancora Information Commissioner's Opinion, *The use of live facial recognition technology by law enforcement in public*

avrebbe dimostrato, né il perché non fossero sufficienti strumenti investigativi meno intrusivi per raggiungere il medesimo risultato, né che «*the choice of location was justified by a specific cause or reasonable suspicion, or both*»[88].

Ma vi è di più. Dopo aver espresso le sue preoccupazioni circa un futuro utilizzo sproporzionato sempre più ampio del riconoscimento facciale, in grado di produrre l'effetto esiziale «*to diminish public confidence in the use of the technology*»[89], l'*ICO* ha ritenuto indispensabile invitare le forze politiche ad adottare «*a statutory binding code of practice to provide further safeguards*»[90], tarate sui pericoli specifici, derivanti dall'utilizzo di *software* di questo tipo. In altre parole, il garante *UK* non ha condiviso l'opinione tranquillizzante della *High Court*, secondo cui sarebbe sufficienti le previsioni già esistenti per tutelare in modo adeguato i diritti dell'uomo dai rischi derivanti dagli strumenti di IA in esame. Tutt'altro contrario: secondo il *Commissioner*, il Governo britannico dovrebbe assumersi la responsabilità di compiere, in tempi rapidi, un vaglio di proporzionalità in astratto sulla possibilità di utilizzare la tecnologia *de qua*, dando vita a un codice di condotta vincolante, volto a stabilire dove, per quali reati e quando le autorità di *law enforcement* possano avvalersi dei *software* di *facial recognition*. L'adozione di un codice siffatto «*would offer law enforcement agencies and the public alike a highly desirable level of clarity and consistency*» e «*would also contribute to the degree of transparency necessary as the use of LFR expands*»[91].

In definitiva, è chiaro come l'*ICO* abbia in questo modo dimostrato di propendere per un approccio assai più garantista rispetto a quello della *High Court*. Per il *Commissioner*, infatti, soltanto l'adozione di un insieme di norme *ad hoc* in materia di riconoscimento facciale sarebbe in grado di limitare gli effetti negativi che degli strumenti così pervasivi, quali quelli in esame, possono produrre sull'individuo e, più in generale, sulle relazioni sociali. A ben vedere, infatti – come hanno affermato in modo convergente l'Agenzia UE per i diritti fondamentali[92] e l'*European Data Protection Supervisor*[93] – non va dimenticato che la tecnologia di *facial recognition*, specie se impiegata in modalità *real-time* come "rete a strascico", nel corso di eventi pubblici, può incidere negativamente sull'esercizio di plurimi diritti fondamentali, quali, ad esempio, il diritto all'associazione e quello di libera manifestazione del pensiero[94], essendovi persino il rischio che le persone sottoposte a mezzi di sorveglianza di massa si sentano «*in a weak and potentially humiliating position*»[95], in spregio al diritto super-primario al rispetto della dignità umana[96]. Una precisa riprova di quanto siffatti pericoli siano tutt'altro che teorici può, del resto, essere tratta dalla recente esperienza delle proteste studentesche di Hong Kong. In tale contesto, infatti, «*the wearing of masks has been a reaction to the use of facial recognition and in turn has been prohibited under a new law*»[97]. Ed è proprio tenuto conto di quest'insieme di rischi che l'Agenzia UE per i diritti fondamentali ha, a sua volta, affermato che costituisce un prerequisito essenziale per utilizzare i sistemi tecnologici in questione il compimento di un «*strict necessity and proportionality test, including a clear legal basis to do so and a legitimate aim*

places, cit., p. 15, laddove il garante è giunto alla conclusione per cui la polizia gallese «*had not ensured that a fair balance between the strict necessity of the processing of sensitive data and the rights of individuals had been struck*».

[88] Al riguardo, v. ancora Information Commissioner's Opinion, *The use of live facial recognition technology by law enforcement in public places*, cit., p. 15.

[89] Information Commissioner's Opinion, *The use of live facial recognition technology by law enforcement in public places*, cit., p. 16.

[90] Sul punto v. Information Commissioner's Opinion, *The use of live facial recognition technology by law enforcement in public places*, cit., p. 21. A riguardo, v. anche Denham (Information Commissioner), *Blog: Live facial recognition technology*, cit. Si erano già espressi in termini simili Babuta e Oswald, *Briefing paper. Data Analytics and Algorithmic Bias in Policing*, 2019, reperibile al presente link.

[91] In proposito, cfr. Information Commissioner's Opinion, *The use of live facial recognition technology by law enforcement in public places*, cit., p. 21.

[92] Cfr. European Union Agency for Fundamental Rights (FRA), *Facial recognition technology,* cit., p. 29 s.

[93] Il rinvio va a Wiewiórowski, *Facial recognition*, cit.

[94] In proposito, si vedano anche Purshouse e Campbell (2019), p. 196, nonché il recente articolo pubblicato da *Amnesty International* sull'utilizzo in Russia della tecnologia in esame: *Russia: Intrusive facial recognition technology must not be used to crackdown on protests*, in *www.amnesty.org*, 31 gennaio 2020. In generale, sul rapporto tra sorveglianza di massa ed esercizio del diritto di associazione si veda lo studio di Starr *et al.* (2008), pp. 251 ss.

[95] Così, European Union Agency for Fundamental Rights (FRA), *Facial recognition technology,* cit., p. 20.

[96] Cfr. ancora European Union Agency for Fundamental Rights (FRA), *Facial recognition technology,* cit., p. 20. Alla luce di ciò, sembra necessario rifiutare la piena equiparazione tra videoriprese semplici e videoriprese *live* con *software* di riconoscimento facciale, suggerita dalla Corte d'oltremanica. Non paiono, invero, esservi dubbi nell'affermare che, nel caso di utilizzo degli algoritmi di *facial recognition*, vi è un'invasione assai più massiccia nella sfera di riservatezza dei singoli (posto che la tecnologia *de qua* permette di associare immediatamente ai loro volti un nome, per il tramite della profilazione di dati biometrici), rispetto alla mera captazione di immagini tramite video.

[97] La citazione è tratta da Wiewiórowski, *Facial recognition*, cit. V. anche Xu Elegant e Mcgregor, *Hong Kong's Mask Ban Pits Anonymity Against the Surveillance State*, in *www.fortune.com*, 4 ottobre 2019.

pursued»[98], pena altrimenti la violazione – tra l'altro – del combinato disposto tra artt. 7 e 8 CDFUE, da un lato, e, dell'art. 52 CDFUE, da un altro lato.

A ogni modo, l'approccio garantista propugnato dall'*ICO* non ha ancora prodotto i risultati sperati. Per rendersi conto di ciò, è sufficiente, del resto, ricordare che nel gennaio 2020 il *Metropolitan Police Service* (*MPS*) ha dichiarato di voler iniziare un programma di ampio utilizzo del *live facial recognition* a Londra[99], senza che però il Governo britannico abbia ancora introdotto l'auspicato codice di condotta sul punto. Com'era prevedibile, l'iniziativa della polizia londinese ha a sua volta suscitato reazioni alquanto accese non solo da parte del garante *UK*, il quale ha pronunciato un nuovo monito, ribadendo la necessità «*to introduce a statutory and binding code of practice for LFR*»[100], ma anche da parte dell'associazione *Big Brother Watch*[101] e di Lord Clement-Jones, «*chair of the House of Lords Artificial Intelligence Committee*»[102]. Quest'ultimo ha, invero, rotto gli indugi, presentando all'inizio di febbraio una proposta di legge, attualmente in discussione presso il Parlamento britannico, tesa a introdurre una moratoria sull'uso ai fini di *law enforcement* del *facial recognition* e ad avviare un percorso di riforma per disciplinare normativamente la tecnologia *de qua*[103].

Indipendentemente dall'*iter* politico che avrà tale *bill*, un dato è chiaro: un prossimo *step* chiave si avrà nel 2021, allorquando la *Court of Appeal* dell'Inghilterra e Galles dovrebbe decidere l'impugnazione che Edward Bridges ha già presentato nei confronti della sentenza della *High Court* qui pubblicata[104]. Nell'attesa che anche questo nuovo (e ancor più) fondamentale *step* si compia, pare utile ricordare che, perlomeno secondo le notizie riportate dalla stampa britannica, le probabilità di accoglimento del ricorso dell'attivista gallese sono tutt'altro che basse, se è vero che il *Lord Justice* Singh, nel momento in cui ha valutato l'ammissibilità dell'appello di Bridges, ha detto che la sua causa ha «*"real prospect of success" on all of his grounds as it "raises such issues of public importance and issues which potentially affect large numbers of people"*»[105]. Chi lo sa, dunque, che non sia proprio una Corte superiore del Regno Unito a far prevalere l'opinione dell'*ICO* su quella della *High Court*, magari – paradossalmente – proprio in virtù di un'interpretazione garantista delle previsioni sulla *privacy*, introdotte nel Regno Unito in attuazione del *data protection package* dell'Unione europea[106].

5. Qualche (breve) notazione conclusiva riguardante l'Italia.

In calce alla ricostruzione del complesso dibattito britannico in tema di mezzi di riconoscimento facciale, siano consentite alcune brevi notazioni concernenti il sistema italiano.

Come si è avuto modo di accennare, anche le autorità di *law enforcement* del nostro Paese possono avvalersi dei *tools* in esame: «risale, infatti, al 2017 la disponibilità da parte della Polizia di Stato, del Sistema automatico di riconoscimento delle immagini»[107] (comunemente

[98] Cfr. European Union Agency for Fundamental Rights (FRA), *Facial recognition technology,* cit., p. 24.

[99] Cfr., in proposito, il seguente annuncio della polizia londinese: *Met begins operational use of Live Facial Recognition (LFR) technology*, in *www.landmobile.co.uk*, 24 gennaio 2020. Al riguardo, cfr. Dodd, *Met police to begin using live facial recognition cameras in London*, in *www.theguardian.com*, 24 gennaio 2020. È, peraltro, d'uopo ricordare che anche la polizia di Londra ha pubblicato sul sito un ampio novero di materiali in tema di riconoscimento facciale (reperibili al seguente link).

[100] Così si è espresso l'*ICO* nel suo *Statement in response to an announcement made by the Metropolitan Police Service on the use of live facial recognition*, al presente link. Si veda anche la risposta del *Biometrics Commissioner* all'annuncio dell'iniziativa della polizia londinese, pubblicata al seguente link.

[101] Cfr., in proposito, la dichiarazione di *Big Brother Watch*, pubblicata al seguente link, dove l'associazione in questione ha annunciato l'intenzione di rafforzare i propri sforzi nell'ambito di una causa legale, presentata già nel 2018 presso l'*High Court* di Londra, al fine di bloccare l'utilizzo da parte della polizia del *facial recognition*. In proposito, v. Mathewson, *Met facial recognition to face legal challenge*, in *www.citymatters.london*, 30 gennaio 2020.

[102] La citazione è tratta da Chertoff, *Facial Recognition Has Its Eye on the U.K.*, cit.

[103] Ci si riferisce all'*Automated Facial Recognition Technology (Moratorium and Review) Bill* [HL] 2019-20, depositato il 4 febbraio 2020, reperibile al seguente link. È peraltro opportuno ricordare che, già dopo la sentenza *Bridges*, Lord Clement-Jones aveva presentato alla Camera dei Lord un primo progetto di riforma in materia, il quale però è stato abbandonato per la fine della legislatura.

[104] Cfr. in proposito Fouzder, *Court of Appeal to hear facial recognition technology challenge*, in *www.lawgazette.co.uk*, 20 novembre 2019.

[105] La citazione è tratta da Dermody, *Facial recognition technology: Ed Bridges appeals human rights ruling*, in *www.bbc.com*, 21 novembre 2019.

[106] Pare utile ricordare che il Regno Unito ha deciso di mantenere in vigore anche dopo la *Brexit* le norme della parte 3 del *Data Protection Act* del 2018, con cui è stata data attuazione alla direttiva 2016/680/UE: in proposito, v. ICO, *Data Protection and Brexit. Law enforcement processing: Five steps to take*, reperibile al presente link.

[107] Cfr. Lopez (2019), p. 240. Il *tool* in questione è stato sviluppato da un'azienda italiana: la Parsec 3.26, «che collabora con il centro di ricerca Cnr Isasi per lo sviluppo di algoritmi di riconoscimento facciale» (così, Pacino, *Come funziona Sari, il sistema di riconoscimento facciale usato dalla Polizia scientifica*, in *www.repubblica.it*, 7 settembre 2018).

noto con l'acronimo SARI), il quale può a sua volta operare tanto «per la ricerca di volti a partire da immagini statiche su banche dati di grandi dimensioni»[108] (c.d. SARI *Enterprise*), quanto *live*, ossia «per il riconoscimento in tempo reale di volti presenti in flussi video provenienti da telecamere»[109] (c.d. SARI *Real-time*)[110].

A tal proposito, va precisato che neppure in Italia è stato finora introdotto un compendio legislativo *ad hoc*, volto a disciplinare i casi e i modi in cui tali mezzi tecnici possono essere utilizzati al fine di reprimere la criminalità. La scelta di dotare degli stessi le autorità di contrasto non è stata, infatti, presa dal Parlamento, ma dal solo Ministro degli Interni, il quale, allorquando ha predisposto il sistema, non ha considerato necessaria l'adozione di fonti normative specifiche in materia. A differenza di quanto è avvenuto nel Regno Unito, una soluzione siffatta ha ricevuto l'avallo del garante per la *privacy* nostrano: quest'ultimo, pur ammettendo che le tecnologie di riconoscimento facciale debbono rispettare la disciplina interna e UE in tema di protezione della *privacy*, ha però escluso che il sistema SARI *Enterprise* presenti qualsivoglia «criticità sotto il profilo della protezione dati»[111].

A quanto risulta, il garante italiano, non si è, invece, ancora pronunciato sulla legittimità dell'utilizzo *Real-Time* di SARI, ossia sulla modalità di captazione assai più intrusiva e delicata, qualificabile come videoripresa "potenziata"[112], poiché capace di profilare in diretta i dati sensibili (e quindi invadere la riservatezza) di un numero quantomai ampio di persone. La mancanza in proposito di un vaglio dell'autorità di tutela dei dati personali pare, a ben vedere, assai problematica, specie tenuto conto delle vistose criticità che attualmente affliggono il sistema di riconoscimento facciale italiano[113].

Ci si riferisce, più precisamente, al fatto che – a quanto risulta – il sistema SARI (*Enterprise* o *Real-Time* che sia) è utilizzabile in tutti gli uffici investigativi della Polizia di Stato, sia centrali, sia periferici[114]. In altre parole, in Italia non vi è come nel Regno Unito una mera attività di sperimentazione del riconoscimento facciale *live* in luoghi ben circoscritti (di cui è dato avviso man mano al pubblico in vari modi). Tutt'al contrario: la tecnologia in questione è, invece, potenzialmente in dotazione delle autorità di *law enforcement* sull'intero territorio nazionale, senza che la collettività sia in alcun modo informata via *web* o in altro modo dell'attività captativa. Alla luce di ciò, non vi sono dubbi nell'affermare che, per ora, il Ministro degli Interni italiano ha fornito alle forze di polizia nostrane poteri e margini di manovra in questa

[108] Così si esprime, testualmente, il seguente documento: Ministero dell'Interno. Dipartimento della pubblica sicurezza, *Capitolato tecnico. Procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini S.A.R.I.,* reperibile al link, p. 7. È d'uopo precisare che le immagini a cui viene applicato il *software* SARI *Enterprise* sono confrontate con i profili facciali estratti dalla banca dati AFIS (*Automated Fingerprint Identification System*), la quale contiene, attualmente, 17.592.769 cartellini fotosegnaletici, corrispondenti a 9.882.490 persone di cui 2.090.064 si riferiscono a cittadini italiani (in questo senso si è espresso il Ministero dell'Interno, nella sua risposta all'interrogazione parlamentare, presentata dopo lo scandalo *Clearview*, dall'On. Sensi. (n. 4-04528), circa il funzionamento del sistema SARI. La riposta *de qua* è reperibile al seguente link).

[109] Cfr., ancora, Ministero dell'Interno. Dipartimento della pubblica sicurezza, *Capitolato tecnico*, cit., p. 7. Anche il sistema SARI *Real-Time*, così come il sopra esaminato *AFR Locate*, confronta i volti presenti nei flussi video con quelli contenuti in una *watchlist* con una grandezza dell'ordine di 100.000 persone (ossia assai più grande di quella utilizzata dalla polizia gallese).

[110] È opportuno ricordare che, esattamente come accade nel Regno Unito, anche il sistema SARI (*Enterprise* o *Real-Time* che sia) fornisce unicamente un *match* tra profili facciali, la cui attendibilità va in ogni caso riscontrata da un operatore di polizia in carne ed ossa. Si tratta quest'ultima, di una garanzia chiave, la quale – tra l'altro – impedisce di poter qualificare le decisioni prese mediante il meccanismo in esame "totalmente automatizzate" ai sensi dell'art. 11 della direttiva 2016/680/UE; e ciò in quanto un essere umano è sempre coinvolto nella fase finale di utilizzo dello strumento.

[111] Ci si riferisce al documento Garante per la protezione dei dati personali, *Sistema automatico di ricerca dell'identità di un volto*, 26 luglio 2018, n. 440, laddove l'autorità *de qua*, dopo aver ricordato che (in virtù del d. lgs. 18 maggio 2018, n. 51 di attuazione della direttiva 2016/680/UE) il trattamento di dati biometrici può avvenire solo laddove sia presente un'adeguata base normativa, ha esplicitamente affermato che per SARI *Enterprise* il requisito in questione «deve ritenersi soddisfatto dalle disposizioni legislative e regolamentari», citate nella scheda n. 19, allegata al decreto del Ministro dell'interno, 24 maggio 2017, recante l'individuazione dei trattamenti di dati personali effettuati con strumenti elettronici e i relativi titolari. Per di più, a detta del garante il requisito della "stretta necessità" del trattamento sarebbe assicurato dalla «funzionalità di tale sistema rispetto alle attività di identificazione svolte dalle forze di polizia». Pare peraltro utile ricordare che, già nel 2014, il garante nostrano aveva adottato delle linee-guida (generali) in materia di riconoscimento biometrico e firma grafometrica, reperibili al seguente link.

[112] Una tale classificazione non vale, ovviamente, per SARI *Enterprise*, il quale svolge una funzione qualificabile in vari modi, a seconda di come il sistema sia utilizzato in concreto. Laddove, infatti, lo stesso serva a meri fini di identificazione di un soggetto, il mezzo *de quo* pare poter rientrare nell'alveo normativo di previsioni quali l'art. 4 T.U.L.P.S. o l'art. 349 c.p.p. Per contro, nel caso in cui SARI *Enterprise* sia applicato a un'immagine già esistente a fini investigativi e/o probatori, esso pare svolgere un'attività riconducibile al *genus* delle individuazioni/ricognizioni fotografiche atipiche, con la peculiarità che il ricognitore in questo caso è una macchina e non un uomo (a quest'ultimo riguardo, cfr., condivisibilmente, Lopez (2019), p. 255).

[113] Un giudizio di tal tipo è espresso anche da Lopez (2019), p. 256 e s.

[114] Da quanto risulta dalla risposta del Ministero dell'Interno alla citata interrogazione parlamentare, presentata dall'On. Sensi, il *tool* in esame è utilizzabile anche dall'Arma dei Carabinieri.

materia assai più ampi rispetto a quelle britanniche (ma anche francesi e tedesche[115]).

È, peraltro, palese come una scelta di tal tipo risulti quantomai critica alla luce dell'art. 10 della direttiva 2016/680/UE, nonché del combinato disposto tra artt. 7, 8 e 52 della Carta di Nizza (e dell'art. 8 CEDU). Difatti, la mancanza di una disciplina legislativa specifica, che stabilisca nel dettaglio per quali reati e a fronte di quali garanzie è possibile attivare il sistema SARI *Real Time*, se collocata in un contesto in cui i *tools* di *facial recognition* sono attivabili in ogni luogo (e senza preavvisare di ciò la collettività) rende assai alto il rischio che la forma di IA in esame sia utilizzata senza rispettare il criterio di "stretta necessità" nella profilazione dei dati personali dei singoli. Per di più, l'assenza di previsioni *ad hoc* sul punto pare porsi in contrasto con quanto ha affermato l'Agenzia UE per i diritti fondamentali. Come si è accennato, quest'ultima ha statuito non solo che l'utilizzo di *software* di riconoscimento facciale può giustificarsi unicamente per fattispecie di reato gravi[116], ma anche che la tecnologia *de qua* deve superare un «*strict necessity and proportionality test, including a clear legal basis*»[117] (in Italia del tutto assente).

Ma i problemi non si fermano qui. A suscitare inevitabili riserve è anche la circostanza per cui, nonostante il sistema SARI sia attivo da circa un biennio, non è finora trapelata alcuna notizia circa l'incidenza percentuale delle comparazioni effettuate con successo mediante lo strumento *de quo*, e, per converso, neppure sul tasso di errore a cui lo stesso statisticamente va incontro[118]. Com'è ovvio, senza possedere queste informazioni è impossibile valutare il livello di affidabilità concreta dell'algoritmo di riconoscimento utilizzato[119], né se eventuali tentativi di affinamento del *software* abbiano o meno avuto successo. Lo si è visto: l'esperienza britannica dimostra come la tecnologia in esame sia in profonda evoluzione e necessiti di aggiornamenti continui per poter funzionare in modo più accurato. Ebbene, sarebbe di primario interesse (anche per le stesse autorità di *law enforcement*) che, esattamente come è avvenuto nel Regno Unito[120], un gruppo di esperti (esterni) potesse accedere a tutta una serie di informazioni pratiche, concernenti il funzionamento del sistema SARI, in modo da valutare che interventi eventualmente mettere in campo per migliorare il *software* di riconoscimento e comprendere se lo stesso sia o meno affetto da *bias* cognitivi discriminatori.

In definitiva, alla luce di queste (e potenzialmente di altre[121]) criticità, non vi sono dubbi nell'affermare che SARI si pone – ad oggi – in contrasto con molti dei principi cristallizzati nella Carta etica sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, stilata sotto l'egida del Consiglio d'Europa[122]. Il canone senz'altro più compromesso è quello di "trasparenza", posto che attualmente – come si è avuto modo di accennare – vi è

[115] Come si desume dal *report* dell'European Union Agency for Fundamental Rights (FRA), *Facial recognition technology,* cit., p. 12 s., tanto le forze di polizia tedesche, quanto quelle francesi, hanno testato l'utilizzo di *software* di riconoscimento facciale, ma «*due to the absence of a legal basis for their deployment, live facial recognition technologies could currently not be used legally in these two countries*». In proposito, è oltretutto utile ricordare che un garante per la protezione dei dati personali tedesco ha scritto un documento sull'applicazione della tecnologia in esame, esprimendo particolari critiche in merito alla mancanza di norme *ad hoc* in materia (ci si riferisce a: Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, *Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg*, reperibile a questo link, p. 31, ove si afferma che «*ohne eine spezielle gesetzliche Regelung ist ein derartiger Eingriff durch Erstellung biometrischer Gesichtstemplates verfassungsrechtlich nicht zulässig*»).

[116] Cfr. European Union Agency for Fundamental Rights (FRA), *Facial recognition technology,* cit., p. 34, ove l'organo in questione ha precisato che la tecnologia in esame «*should be strictly limited to combatting terrorism and other forms of serious crime, or to detect missing people and victims of crime*».

[117] In proposito, v. European Union Agency for Fundamental Rights (FRA), *Facial recognition technology,* cit., p. 24. Cfr. anche il Libro bianco del 19 febbraio 2020 della Commissione europea, *sull'intelligenza artificiale*, cit., p. 24, ove si afferma che «conformemente alle vigenti norme dell'UE in materia di protezione dei dati e alla Carta dei diritti fondamentali, l'IA può essere utilizzata a fini di identificazione biometrica remota unicamente ove tale uso sia debitamente giustificato, proporzionato e soggetto a garanzie adeguate».

[118] Si veda al riguardo Lopez (2019), p. 246.

[119] In ragione di ciò, coglie senz'altro nel segno quella dottrina (Lopez (2019), p. 257), la quale ha affermato che «in considerazione dei molti quesiti sollevati sul funzionamento del S.A.R.I., tuttora senza risposta, la garanzia della sua affidabilità ricognitiva specie nei casi di sovrapponibilità altamente incerta è fievole, in quanto esito di una procedura "blindata" e di dati ignoti».

[120] Ci si riferisce, sia alla citata analisi dell'Università di Cardiff sull'utilizzo da parte della polizia gallese dei *software* in questione (Davies, Innes, Dawson, *An Evaluation of South Wales Police's Use of Automated Facial Recognition*, cit.), sia alla ricerca – compiuta da Fussey e Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, cit. – concernente l'applicazione del riconoscimento facciale da parte delle autorità di contrasto londinesi.

[121] Un'altra questione assai delicata riguarda la mancanza di una fonte normativa, che stabilisca sulla base di quali parametri un soggetto possa essere legittimamente inserito nelle *watchlist* di soggetti ricercati tramite SARI *Real-Time*.

[122] Il rinvio va alla Carta etica europea, sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, adottata dalla CEPEJ il 3-4 dicembre 2018, CEPEJ (2018) 14. Per un commento all'atto in questione, cfr. Barbaro (2018), pp. 189 ss. e Quattrocolo (2018). In realtà, criticità analoghe emergono anche nei confronti di altri atti analoghi, quali, ad esempio, gli *Orientamenti etici per un'IA affidabile*, pubblicati l'8 aprile 2019, sotto l'egida UE dal Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale, istituito dalla Commissione europea nel giugno 2018, nonché la raccomandazione dell'OCSE del 22 maggio del 2019 sull'intelligenza artificiale.

un assai preoccupante velo di oscurità sull'effettivo funzionamento del sistema. La speranza pertanto è quella per cui questa linea di tendenza subisca una netta inversione e che il Governo faccia al più presto piena chiarezza sull'utilizzo che nella prassi sta vendendo fatto dalle autorità di contrasto dei *software* di riconoscimento facciale[123]. Un tanto permetterebbe non solo alla collettività di meglio valutare il grado di rispetto dei diritti fondamentali fornito dai meccanismi di *facial recognition* nostrani, ma soprattutto alle forze politiche di predisporre con cognizione di causa un (assai auspicabile) intervento normativo in materia, che vada a colmare le evidenti problematiche che affliggono SARI[124]. Certo, la circostanza per cui il legislatore italiano – in modo assai criticabile – non abbia mai regolato non solo altri strumenti investigativi tecnologici di nuovo conio[125], ma persino le semplici videoriprese investigative[126] (senza riconoscimento facciale) non fa ben sperare sul fatto che la lacuna più insidiosa, concernente l'utilizzazione *live* del *software* in esame, venga colmata in tempi rapidi.

Indipendente da ciò, risulta quantomai urgente che pure in Italia – così come nel Regno Unito – tanto la dottrina, quanto – soprattutto – la giurisprudenza e il garante per la protezione dei dati personali facciano la loro parte, dando vita a un dibattito costruttivo, volto a individuare un corretto bilanciamento tra esigenze di sicurezza e rispetto dei diritti fondamentali, allorquando siano utilizzate tecnologie, come quella in esame, in grado di invadere la *privacy* di una sfera potenzialmente enorme di individui. Permanere nell'attuale immobilismo non può, del resto, che portare a effetti controproducenti. Non è difficile prevedere, infatti, che, ben presto, i *facial recognition systems* dovranno superare il vaglio tanto dei giudici di Strasburgo, quanto del Lussemburgo, con tutto ciò che potrà comportare in termini di contenzioso per un sistema, come quello italiano, che in questa materia risulta tra i meno garantisti d'Europa[127].

Bibliografia

Barbaro, Clementina (2018): "Uso dell'intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo?", *Questione giustizia*, 4, pp. 189-195.

Basile, Fabio (2019): "Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine", *Diritto penale contemporaneo*, 23 settembre 2019.

Bene, Teresa (2019): "Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali", in Scalfati, Adolfo (editor), *Le indagini atipiche*, (Torino, Giappichelli, 2ª ed.), 443-464.

Bennett, Kanya A. (2002): "Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveillance Systems", *North Carolina Journal of Law & Technology*, pp. 151-174.

Bonini, Valentina (2019): "Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa", *Processo penale e giustizia*, pp. 338-348.

[123] A questo proposito, è stata senz'altro un'occasione perduta la più volte citata risposta all'interrogazione parlamentare dell'On. Sensi. Dal canto suo, infatti, il Viminale si è limitato a fornire poche (e vaghe) spiegazioni con riguardo al funzionamento del solo sistema SARI *Enterprise*, chiarendo, da un lato, che ad oggi quest'ultimo attinge i profili facciali da sottoporre a confronto unicamente dalla banca dati AFIS e non da altre fonti (come, invece, era stato ventilato da alcuni, tra cui, ad es. Lopez (2019), p. 246) e, da un altro lato, che le immagini utilizzate per le ricerche sono acquisite dagli uffici di polizia nell'ambito di indagini penali, oppure sono trasmesse dal Servizio di Cooperazione Internazionale di Polizia. Per contro, il Ministero non solo non ha fatto alcun riferimento a SARI *Real-Time*, ma oltretutto non ha divulgato nessun dato circa l'utilizzo che nella prassi si è fatto finora di entrambi i meccanismi in esame.

[124] Come si è visto, all'estero non mancano modelli da cui le forze politiche potrebbero trarre ispirazione. Ci si riferisce, ad esempio, alla citata proposta normativa attualmente in discussione negli USA, denominata "*Facial Recognition Technology Warrant Act*".

[125] Si pensi, solo per fare un esempio, al pedinamento elettronico tramite GPS (sul quale, cfr., tra i molti, Bene, (2019), pp. 443 ss.; Fanuele (2019); Filippi (2012); Iovene (2012), pp. 3556 ss.).

[126] Sul tema, com'è noto, la letteratura è vastissima. Per reperire i dovuti riferimenti dottrinali e giurisprudenziali, si consenta il rinvio, oltre ai recenti lavori di Bonini (2019), pp. 338 ss. e Triggiani (2019), pp. 161 ss., alla voce di Camon (2013), pp. 133 ss.

[127] Si veda, a riguardo, il recente studio di Comparitech, *Data privacy laws & government surveillance by country: Which countries best protect their citizens?*, in *www.comparitech.com*, 15 ottobre 2019, il quale afferma che l'Italia sarebbe lo Stato dell'intera area UE con più lacune in materia di *privacy*, anche a causa dell'«*extensive CCTV use (including with facial recognition)*». Per una sintesi di tale studio, cfr. l'articolo di Tremolada, Privacy, *Italia ultima in Europa nel riconoscimento facciale, Garante poco "attivo"*, in *www.infodata.ilsole24ore.com*, 25 ottobre 2019.

Bowyer, Kevin W. (2004): "Face Recognition Technology: Security versus Privacy", *IEEE Technology and Society Magazine*, pp. 9-20.

Brogan, John J. (2002): "Facing the Music: The Dubious Constitutionality of Facial Recognition Technology", *Hasting Communications and Entertainment Law Journal*, pp. 65-96.

Camon, Alberto (2013): "Captazione di immagini (diritto processuale penale)", *Enciclopedia del diritto*, Annali, VI, (Milano, Giuffrè), pp. 133-149.

Contissa, Giuseppe, Lasagni Giulia, Sartor Giovanni (2019): "Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo", *Diritto di internet*, pp. 619-634;

Costanzi, Claudio (2018): "La matematica del processo: oltre le colonne d'Ercole della giustizia penale", *Questione giustizia*, 4, pp. 166-188.

D'Agostino, Luca (2019): "Gli algoritmi predittivi per la commisurazione della pena", *Diritto penale contemporaneo – Rivista trimestrale*, 2, pp. 354-373.

Di Paolo, Gabriella (2008): *Tecnologie del controllo e prova penale. L'esperienza statunitense e spunti per la comparazione* (Padova, Cedam).

Fanuele, Chiara (2019): *La localizzazione satellitare nelle investigazioni penali*, (Milano, Wolters Kluwer-Cedam).

Filippi, Leonardo (2012): "Il GPS è una prova incostituzionale? Domanda provocatoria, ma non troppo, dopo la sentenza Jones della Corte suprema U.S.A.", *Arch. pen. online*, 1.

Fretty, Douglas A. (2011): "Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights in Public Places", *Virginia Journal of Law & Technology*, pp. 430-463.

Gates, Kelly (2006): "Identifying the 9/11 "Faces of terror". The promise and problem of facial recognition technology", *Cultural Studies*, pp. 417-440.

Gialuz, Mitja (2019): "Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei *risk assessment tools* tra Stati Uniti ed Europa", *Diritto penale contemporaneo*, 29 maggio 2019.

Gillespie, Alisdair e Weare, Siobhan (2019): *The English Legal System*, (Oxford, Oxford University Press).

González Cano, Isabel (2019): "Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680", *Revista Brasileira de Direito Processual Penal*, pp. 1331-1383.

Iovene, Federica (2012): "Pedinamento satellitare e diritti fondamentali della persona", *Cassazione penale*, pp. 3556-3565.

Iraola, Roberto (2003): "Lights, Camera, Action! – Surveillance Cameras, Facial Recognition Systems and the Constitution", *Loyola Law Review*, pp. 773-808.

Kotsoglou, Kyriakos N. e Oswald, Marion (2020): "The Long Arm of the Algorithm? Automated Facial Recognition as evidence and trigger for police intervention", *Forensic Science International: Synergy*, pp. 86-89.

Maldonato, Lucia (2019): "Algoritmi predittivi e discrezionalità del giudice: una nuova sfida per la giustizia penale", *Diritto penale contemporaneo – Rivista trimestrale*, 2, pp. 401-416.

Mattei, Ugo (2010): *Il modello di* common law (Torino, Giappichelli, 3ª ed.).

Milligan, Christopher (1999): "Facial recognition technology, video surveillance, and privacy", *Southern California Interdisciplinary Law Journal*, pp. 295-333.

McCoy, Susan (2002): "O' Big Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology", *The John Marshall Journal of Information Technology & Privacy Law*, pp. 471-493.

Murphy, Julian R. (2018): "Chilling: The Constitutional Implications of Body-Worn Cameras and Facial Recognition Technology at Public Protests", *Washington and Lee Law Review Online*, 2018, pp. 1-32.

Nieva-Fenoll, Jordi (2019): *Intelligenza artificiale e processo* (Giappichelli, Torino).

Occhiuzzi, Barbara (2019): "Algoritmi predittivi: alcune premesse metodologiche", *Diritto penale contemporaneo*, 2, pp. 391-400.

Lopez, Rita (2019): "La rappresentazione facciale tramite *software*", in Scalfati, Adolfo (editor), *Le indagini atipiche*, (Torino, Giappichelli, 2ª ed.), pp. 239-257.

Pagallo, Ugo e Quattrocolo, Serena (2018): "The Impact of AI on criminal law, and its twofold procedures", in Barfield, Woodrow e Pagallo, Ugo (eds.) *Research Handbook on the Law of Artificial Intelligence* (Northampton, Elgar), pp. 385-410.

Parodi, Cesare e Sellaroli, Valentina (2019): "Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco", *Diritto penale contemporaneo*, 16 giugno 2019.

Purshouse, Joe e Campbell, Liz (2019): "Privacy, Crime Control and Police Use of Automated Facial Recognition Technology", *Criminal Law Review*, pp. 188-204.

Quattrocolo, Serena (2019a): "An introduction to AI and criminal justice in Europe", *Revista Brasileira de Direito Processual Penal*, pp. 1519 -1554.

Quattrocolo, Serena (2019b): "Equità del processo penale e *automated evidence* alla luce della Convenzione europea dei diritti dell'uomo", *Revista Ítalo-Española de Derecho Procesal*, 2, pp. 1-17.

Quattrocolo, Serena (2019c): "Equo processo penale e sfide della società algoritmica", *BioLaw Journal*, 2019, 1, pp. 135-144.

Quattrocolo, Serena (2019d): "Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"", *Cassazione penale*, pp. 1748-1765.

Quattrocolo, Serena (2018): "Intelligenza artificiale e giustizia: nella cornice della Carta etica europea gli spunti per un'urgente discussione tra scienze penali e informatiche", *www.lalegislazionepenale.it*, 18 dicembre 2018.

Riccio, Giuseppe (2019): "Ragionando su intelligenza artificiale e processo penale", *Archivio penale online*, 3.

Ringrose, Katelyn (2019): "Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns", *Virginia Law Review Online*, pp. 57-66.

Sacchetto, Ernestina (2019): "Spunti per una riflessione sul rapporto fra biometria e processo penale", *Diritto penale contemporaneo – Rivista Trimestrale*, 2, p. 465-480.

Starr, Amory, Fernandez, Luis, Amster, Randall, Wood, Lesley, Caro, Manuel J. (2008): "The Impact of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis", *Qualitative Sociology*, pp. 251-270.

Thornburg, Robert H. (2002): "Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment", *The John Marshall Journal of Information Technology & Privacy Law*, 2002, pp. 321-346.

Traversi, Alessandro (2019): "Intelligenza artificiale applicata alla giustizia: ci sarà un giudice *robot*?", *www.questionegiustizia.it*, 10 aprile 2019.

Triggiani, Nicola (2019): "Le videoriprese investigative e l'uso dei droni", in Scalfati, Adolfo (editor), *Le indagini atipiche*, (Torino, Giappichelli, 2ª ed.), pp. 161-190.

Valli, Roberto V.O. (2019): "Sull'utilizzabilità processuale del Sari: il confronto automatizzato di volti rappresentati in immagini", *Il Penalista*, 16 gennaio 2019.

Woodward, John D. (1999): "Biometrics: identifying law & policy concerns", in Jain, Anil, Bolle, Ruud, Pankanti, Sharath (eds.), *Biometrics: Personal Identification in Networked Society* (Boston, Dordrecht, London, Springer), pp. 385-405.

Woodward, John D (1997): "Biometric scanning, law & policy: identifying the concerns drafting the biometric blueprint", *University of Pittsburgh Law Review*, pp. 97-155.

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

Ziroldi, Alberto (2019): "Intelligenza artificiale e processo penale tra norme, prassi e prospettive", *www.questionegiustizia.it*, 18 ottobre 2019.

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

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