

C J N

Diritto Penale Contemporaneo

R I V I S T A T R I M E S T R A L E

REVISTA TRIMESTRAL DE DERECHO PENAL
A QUARTERLY REVIEW FOR CRIMINAL JUSTICE



Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione

IX Corso di formazione interdottorale di Diritto e Procedura penale 'Giuliano Vassalli' per dottorandi e dottori di ricerca

(AIDP Gruppo Italiano, Siracusa International Institute for Criminal Justice and Human Rights – Siracusa, 29 novembre - 1° dicembre 2018)

ISSN 2240-7618

2/2019

EDITOR-IN-CHIEF

Gian Luigi Gatta

EDITORIAL BOARD

Italy: Antonio Gullo, Guglielmo Leo, Luca Luparia, Francesco Mucciarelli, Francesco Viganò
Spain: Jaime Alonso-Cuevillas, Sergi Cardenal Montraveta, David Carpio Briz, Joan Queralt

Jiménez

Chile: Jaime Couso Salas, Mauricio Duce Julio, Héctor Hernández Basualto, Fernando Londoño Martínez

MANAGING EDITOR

Carlo Bray

EDITORIAL STAFF

Alberto Aimi, Enrico Andolfatto, Enrico Basile, Javier Escobar Veas, Stefano Finocchiaro, Elisabetta Pietrocarlo, Tommaso Trincherà, Stefano Zirulia

EDITORIAL ADVISORY BOARD

Rafael Alcacer Guirao, Alberto Alessandri, Giuseppe Amarelli, Ennio Amodio, Coral Arangüena Fanego, Lorena Bachmaier Winter, Roberto Bartoli, Fabio Basile, Hervé Belluta, Alessandro Bernardi, Carolina Bolea Bardón, David Brunelli, Silvia Buzzelli, Alberto Cadoppi, Pedro Caeiro, Michele Caianiello, Lucio Camaldo, Stefano Canestrari, Francesco Caprioli, Claudia Cárdenas Aravena, Raúl Carnevali, Marta Cartabia, Elena Maria Catalano, Mauro Catenacci, Massimo Ceresa Gastaldo, Mario Chiavario, Mirentxu Corcoy Bidasolo, Cristiano Cupelli, Norberto Javier De La Mata Barranco, Angela Della Bella, Cristina de Maglie, Gian Paolo Demuro, Miguel Díaz y García Conlledo, Ombretta Di Giovine, Emilio Dolcini, Jacobo Dopico Gomez Áller, Patricia Faraldo Cabana, Silvia Fernández Bautista, Javier Gustavo Fernández Terruelo, Marcelo Ferrante, Giovanni Fiandaca, Gabriele Fornasari, Novella Galantini, Percy García Caveró, Loredana Garlati, Mitja Gialuz, Glauco Giostra, Víctor Gómez Martín, José Luis Guzmán Dalbora, Ciro Grandi, Giovanni Grasso, Giulio Illuminati, Roberto E. Kostoris, Máximo Langer, Juan Antonio Lascurain Sánchez, Maria Carmen López Peregrín, Sergio Lorusso, Ezequiel Malarino, Francisco Maldonado Fuentes, Stefano Manacorda, Juan Pablo Mañalich Raffo, Vittorio Manes, Grazia Mannozi, Teresa Manso Porto, Luca Marafioti, Joseph Margulies, Enrico Marzaduri, Luca Maserà, Jean Pierre Matus Acuña, Anna Maria Maugeri, Oliviero Mazza, Iván Meini, Alessandro Melchionda, Chantal Meloni, Melissa Miedico, Vincenzo Militello, Santiago Mir Puig, Fernando Miró Linares, Vincenzo Mongillo, Renzo Orlandi, Francesco Palazzo, Carlenrico Paliero, Michele Papa, Raphaële Parizot, Claudia Pecorella, Marco Pelissero, Lorenzo Picotti, Paolo Pisa, Oreste Pollicino, Domenico Pulitanò, Tommaso Rafaraci, Paolo Renon, Mario Romano, María Ángeles Rueda Martín, Carlo Ruga Riva, Stefano Ruggeri, Francesca Ruggieri, Marco Scoletta, Sergio Seminara, Paola Severino, Nicola Selvaggi, Rosaria Sicurella, Jesús María Silva Sánchez, Carlo Sotis, Giulio Ubertis, Inma Valeije Álvarez, Antonio Vallini, Paolo Veneziani, Costantino Visconti, Javier Willenmann von Bernath, Francesco Zacchè

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.

Il lettore può leggere, condividere, riprodurre, distribuire, stampare, comunicare al pubblico, esporre in pubblico, cercare e segnalare tramite collegamento ipertestuale ogni lavoro pubblicato su "Diritto penale contemporaneo – Rivista trimestrale", con qualsiasi mezzo e formato, per qualsiasi scopo lecito e non commerciale, nei limiti consentiti dalla licenza Creative Commons - Attribuzione - Non commerciale 3.0 Italia (CC BY-NC 3.0 IT), in particolare conservando l'indicazione della fonte, del logo e del formato grafico originale, nonché dell'autore del contributo.

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 con 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 protección 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.

Visitors to the site may share, reproduce, distribute, print, communicate to the public, search and cite using a hyperlink every article published in the journal, in any medium and format, for any legal non-commercial purposes, under the terms of the Creative Commons License - Attribution – Non-commercial 3.0 Italy (CC BY-NC 3.0 IT). The source, logo, original graphic format and authorship must be preserved.

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](#)).

IL DIRITTO PENALE
NEL CYBERSPAZIO

*EL DERECHO PENAL
EN EL CIBERESPACIO*

*CRIMINAL LAW
IN CYBERSPACE*

Neutralization Theory: Criminological Cues for Improved Deterrence of Hacker Crimes	1
<i>“Teoría de la neutralización”: tra prevención e repressione del cybercrime</i>	
<i>“Teoría de la neutralización”: Entre prevención y represión del cibercrimen.</i>	
Marcello Sestieri	

«Send nudes» Il trattamento penalistico del sexting in considerazione dei diritti fondamentali del minore d'età	9
<i>El tratamiento penal del sexting en consideración a los derechos fundamentales de los menores de edad</i>	
<i>The Criminalisation of Sexting Involving Underage Victims</i>	
Domenico Rosani	

Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme online	33
<i>Los efectos de la automatización en los modelos de responsabilidad: el caso de las plataformas online</i>	
<i>The Effects of Automation on Imputation Models: the Case of Online Platforms</i>	
Beatrice Panattoni	

DIRITTO PENALE E
LIBERTÀ DI ESPRESSIONE
IN INTERNET

*EL DERECHO PENAL Y LA
LIBERTAD DE EXPRESIÓN EN
INTERNET*

*CRIMINAL LAW AND
FREEDOM OF EXPRESSION
ON THE INTERNET*

Istanze di criminalizzazione delle fake news al confine tra tutela penale della verità e repressione del dissenso	60
<i>La criminalización de las fake news entre al confín entre tutela penal de la verdad y represión del disenso</i>	
<i>Criminalisation of Fake News Between the Protection of Truth and the Suppression of Dissent</i>	
Anna Costantini	

Il volto dei reati di opinione nel contrasto al terrorismo internazionale al tempo di Internet	81
<i>El rostro de los delitos de opinión en la lucha contra el terrorismo internacional en la época de Internet</i>	
<i>The Face of Word Crimes in the Fight Against International Terrorism at the Time of the Internet</i>	
Paolo Cirillo	

<p><i>FINANCIAL</i> <i>CYBERCRIME</i></p> <p><i>CIBERCRIMEN</i> <i>FINANCIERO</i></p> <p><i>FINANCIAL</i> <i>CYBERCRIME</i></p>	<p>Crowdfunding @ ICOs: esigenze di prevenzione del rischio di commissione di reati nell'era della digital economy 101</p> <p><i>Crowdfunding @ ICOs: exigencias de prevención del riesgo de comisión de delitos en la era de la economía digital</i></p> <p><i>Crowdfunding @ ICOs: Commission Risk Prevention Needs of Crimes in the Era of the Digital Economy</i></p> <p>Antonietta di Lernia</p>
	<p>La tutela penale del segreto commerciale in Italia. 112</p> <p>Fra esigenze di adeguamento e possibilità di razionalizzazione</p> <p><i>La tutela penal del secreto comercial en Italia.</i></p> <p><i>Entre exigencias de adecuación y posibilidades de racionalización</i></p> <p><i>The Protection of Trade Secret under Italian Criminal Law.</i></p> <p><i>Between Needs for Adequacy and Options for Rationalization</i></p> <p>Riccardo Ercole Omodei</p>
	<p>L'abuso di mercato nell'era delle nuove tecnologie. 129</p> <p>Trading algoritmico e principio di personalità dell'illecito penale</p> <p><i>Abuso del mercado en la era de las nuevas tecnologías.</i></p> <p><i>Trading algorítmico y principio de responsabilidad penal personal</i></p> <p><i>Market Abuse in the Age of New Technologies.</i></p> <p><i>Algorithmic Trading and Principle of Individual Criminal Responsibility</i></p> <p>Marta Palmisano</p>
	<p>Gli strumenti di prevenzione nazionali ed europei in materia di valute virtuali e riciclaggio 148</p> <p><i>Los instrumentos de prevención nacional y europeos en materia de monedas virtuales y lavado de activos</i></p> <p><i>Domestic and European Preventative Instruments Concerning Virtual Currencies and Money Laundering</i></p> <p>Cristina Ingrao</p>
	<p>Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione 159</p> <p><i>Las monedas virtuales y los ontológicos riesgos de lavado de activos: técnicas de represión.</i></p> <p><i>Virtual currencies and the endemic risk of money laundering: repression techniques</i></p> <p>Fabiana Pomes</p>

<p>LA TUTELA PENALE DELLA PRIVACY NEL CYBERSPAZIO</p> <p><i>LA TUTELA PENAL DE LA PRIVACIDAD EN EL CIBERESPACIO</i></p> <p><i>CRIMINAL LAW AND THE PROTECTION OF PRIVACY IN CYBERSPACE</i></p>	<p>I limiti della tutela penale del trattamento illecito dei dati personali nel mondo digitale</p> <p><i>Los límites de la tutela penal del tratamiento ilícito de datos personales en el mundo digital</i></p> <p><i>Limits to Criminalization of Unlawful Data Processing in the Digital World</i></p> <p>Salvatore Orlando</p>	<p>178</p>
	<p>Il compendio sanzionatorio della nuova disciplina privacy sotto la lente del <i>ne bis in idem</i> sovranazionale e della Costituzione</p> <p><i>El compendio sancionatorio de la nueva regulación de la privacidad bajo la lente del ne bis in idem internacional y de la Constitución italiana</i></p> <p><i>The Sanctioning System for Privacy-Related Infringements from the Supranational Ne Bis In Idem and the Italian Constitution Perspectives</i></p> <p>Ludovica Deaglio</p>	<p>201</p>
	<p><i>Eternal Sunshine of the Spotless Crime.</i></p> <p>Informazione e oblio nell'epoca dei processi su internet</p> <p><i>Eternal Sunshine of the Spotless Crime.</i></p> <p><i>Información y olvido en la época de los procesos de internet</i></p> <p><i>Eternal Sunshine of the Spotless Crime.</i></p> <p><i>The Right to Information and the Right to be Forgotten in Times of Trials by Media</i></p> <p>Edoardo Mazzanti</p>	<p>212</p>
	<p>La moltiplicazione dei garanti nel settore della tutela dei dati personali: riflessi penalistici del GDPR</p> <p><i>La multiplicación de las garantías en el sector de la tutela de los datos personales: Reflexiones penalísticas del GDPR</i></p> <p><i>The Multiplication of Responsibilities in the Personal Data Protection Area: Criminal Law Implications of the GDPR</i></p> <p>Gaia Fiorinelli</p>	<p>239</p>
	<p><i>Corporate liability e compliance in the cyber privacy crime:</i></p> <p>il nuovo “modello organizzativo privacy”</p> <p><i>Responsabilidad corporativa y compliance en el delito de privacidad cibernética: El nuevo “modelo organizativo de privacidad”</i></p> <p><i>Corporate Liability and Compliance in the Cyber Privacy Crime: the New “Privacy Organizational Model”</i></p> <p>Valentina Aragona</p>	<p>251</p>

SICUREZZA INFORMATICA, COMPLIANCE E PREVENZIONE DEL RISCHIO DI REATO <i>SEGURIDAD INFORMÁTICA, COMPLIANCE Y PREVENCIÓN DEL RIESGO DE DELITOS</i> <i>IT SECURITY, COMPLIANCE AND CRIME PREVENTION</i>	<hr/> I discorsi d'odio nell'era digitale: quale ruolo per l'internet service provider? <i>Los discursos de odio en la era digital: ¿Cuál es el rol del proveedor de servicios de internet?</i> <i>Hateful Speech in the Digital Era: Which Role for the ISP?</i> Valérie Nardi	268
	<hr/> Big Data Analytics e compliance anticorruzione Profili problematici delle attuali prassi applicative e scenari futuri <i>Análisis de Big Data y compliance anticorrupción</i> <i>Cuestiones críticas de la práctica actual y escenarios futuros</i> <i>Big Data Analytics and Anti-corruption Compliance</i> <i>Critical Issues of Current Practice and Future Scenarios</i> Emanuele Birritteri	289
	<hr/> La partita del diritto penale nell'epoca dei "drone-crimes" <i>El partido del derecho penal en la era de los "delitos de dron"</i> <i>The Criminal Law Match in the Era Of "Drone-Crimes"</i> Carla Cucco	304
	<hr/> Profili penalistici delle self-driving cars <i>Cuestiones de derecho penal en relación a los vehículos de conducción autónoma</i> <i>Self-driving Cars and Criminal Law</i> Alberto Cappellini	325
	<hr/> Gli algoritmi predittivi per la commisurazione della pena. A proposito dell'esperienza statunitense nel c.d. evidence-based sentencing <i>Los algoritmos predictivos para la determinación de la pena. A propósito de la experiencia estadounidense del "evidence-based sentencing"</i> <i>Predictive Algorithms for Sentencing. The US Experience of the So-Called Evidence-Based Sentencing</i> Luca D'Agostino	354
	<hr/> Banche dati, attività informativa e predittività. La garanzia di un diritto penale del fatto. <i>Bases de datos, actividades de información y predictibilidad. La garantía de un derecho penal del hecho</i> <i>Databases, Information Activities and Prediction. The Safeguard of Fact-related Criminal Law</i> Pietro Sorbello	374

NUOVE TECNOLOGIE E PROCESSO PENALE <i>NUEVAS TECNOLOGÍAS Y PROCESO PENAL</i> <i>NEW TECHNOLOGIES AND CRIMINAL PROCEDURE</i>	Algoritmi predittivi: alcune premesse metodologiche 391 <i>Algoritmos predictivos: algunas premisas metodológicas</i> <i>The 'multi-faceted' brain of predictive algorithms.</i> Barbara Occhiuzzi
	Algoritmi predittivi e discrezionalità del giudice: una nuova sfida per la giustizia penale 401 <i>Algoritmos predictivos y discrecionalidad del juez: un nuevo desafío para la justicia penal</i> <i>Predictive Algorithms and Judicial Discretion: a New Challenge for Criminal Justice</i> Lucia Maldonato
	Le nuove indagini tecnologiche e la tutela dei diritti fondamentali. L'esperienza del captatore informatico 417 <i>Las nuevas tecnologías de investigación y la tutela de los derechos fundamentales. La experiencia del software espía</i> <i>New IT-based Investigations and Protection of Fundamental Rights.</i> <i>The Case of Spy-software</i> Gaia Caneschi
	Il controllo occulto e continuativo come categoria probatoria: premesse teoriche di una sistematizzazione 430 <i>El control oculto y continuado como categoría probatoria: premisas teóricas de una sistematización</i> <i>The Hidden and Continous Control as Evidentiary Notion: Theoretical Premises for a Systematic Analysis</i> Fabio Nicolichia
	L'accesso transfrontaliero all'electronic evidence, tra esigenze di effettività e tutela dei diritti 439 <i>El acceso transfronterizo a evidencia electrónica, entre exigencias de efectividad y tutela de derechos</i> <i>Transnational Access to Electronic Evidence Between Effectiveness and the Need to Protect Rights</i> Veronica Tondi

L'utilizzo dello <i>smartphone</i> alla guida nei delitti di omicidio e lesioni colpose stradali: l'accertamento processuale della colpa attraverso i c.d. <i>file di log</i>.	456
<i>El uso del <i>smartphone</i> al momento de conducir en los delitos de asesinato y lesiones culposas: la verificación procesal de la culpa a través del archivo de registro</i>	
<i>The Usage of Smartphones While Driving and The Road/Traffic-Related Crimes of Manslaughter and Personal Negligence-Based Injuries: the Assessment of Negligence in Court Through the So-Called Log Files.</i>	
Giacomo Maria Evaristi	

Spunti per una riflessione sul rapporto fra biometria e processo penale	465
<i>Ideas para reflexionar sobre la relación entre biometría y proceso penal</i>	
<i>Ideas for a Reflection on the Relationship Between Biometrics and Criminal Trial</i>	
Ernestina Sacchetto	

NUOVE TECNOLOGIE E PROCESSO PENALE
NUEVAS TECNOLOGÍAS Y PROCESO PENAL
NEW TECHNOLOGIES AND CRIMINAL PROCEDURE

Spunti per una riflessione sul rapporto fra biometria e processo penale*

Ideas para reflexionar sobre la relación entre biometría y proceso penal

Ideas for a Reflection on the Relationship Between Biometrics and Criminal Trial

ERNESTINA SACCHETTO

Dottoranda di ricerca in "Diritti e Istituzioni" presso l'Università degli studi di Torino
ernestina.sacchetto@unito.it

PROVA SCIENTIFICA

PRUEBA PERICIAL

FORENSIC EVIDENCE

ABSTRACTS

Lo scritto si propone di offrire una panoramica dei caratteri principali della disciplina biometrica e di alcune problematiche emergenti dalla sua applicazione nel processo penale: a partire da necessarie precisazioni terminologiche si passerà all'esposizione del metodo biometrico corredato dalle relative misure di accuratezza che i vari sistemi di riconoscimento possono presentare in livelli differenti. Ci si prefiggerà altresì di illustrare le più diffuse tecnologie di identificazione e autenticazione tra cui le impronte digitali, il riconoscimento del volto, la misurazione dell'iride e della retina, la voce, l'andatura e la prova genetica. Tali sistemi biometrici presentano sicuri vantaggi applicativi non solo in ambiti privati (dall'accesso a determinati luoghi al godimento di vari servizi) ma anche nell'ambito processuale penale, in termini investigativi e probatori. Dopo aver fatto cenno allo "stato dell'arte" della prova scientifica, si focalizzerà l'attenzione su alcune possibili criticità emergenti dal rapporto fra la scienza biometrica e il processo penale. In primis, si rileva una confusione terminologica, dettata dall'assenza di una definizione unica, tanto in letteratura quanto in giurisprudenza, dell'aggettivo "biometrico". In secondo luogo, ad oggi non vi sarebbero ancora risultati univoci in termini di affidabilità di tali tecniche di riconoscimento e una riflessione complessiva va avviata con riguardo alla compatibilità con i principi costituzionali e le garanzie processuali.

El presente artículo tiene por finalidad ofrecer un panorama de las principales características de la disciplina biometría y de algunos problemas emergentes respecto a su aplicación en el proceso penal. Luego de algunas necesarias precisiones terminológicas, se expone en general el método biométrico, describiendo las principales tecnológicas de identificación y autenticación, entre las cuales se encuentra la huella digital, el reconocimiento facial, la medida del iris y retina, el reconocimiento de voz y la prueba genética. Estos sistemas biométricos presentan ventajas no solo en el ámbito privado, sino que también en el contexto del proceso penal, en términos investigativos y probatorios. Después de describir el "estado del arte" de la prueba científica, el trabajo se concentra en algunos posibles problemas relativos a la relación entre la ciencia biométrica y el proceso penal. En primer lugar, se evidencia una confusión terminológica, dictada por la ausencia de una definición única, tanto en la literatura como en la jurisprudencia, del adjetivo "biométrico". En segundo lugar, hasta la fecha todavía no existen

* I miei più sentiti ringraziamenti vanno agli organizzatori del nono corso di formazione interdotto di Diritto e Procedura Penale "Giuliano Vassalli" per Dottorandi e Dottori di ricerca (Siracusa International Institute in collaborazione con il gruppo italiano dell'Associazione Internazionale di Diritto Penale - AIDP) intitolato "Nuove frontiere tecnologiche e sistema penale - Sicurezza informatica, strumenti di repressione e tecniche di prevenzione" nonché ai tutori del mio progetto di ricerca, il Professor Francesco Caprioli e la Professoressa Barbara Lavarini. Alla Prof.ssa Serena Quattrococo va la mia profonda riconoscenza per il Suo contributo alle riflessioni confluente nel presente lavoro.

resultados inequívocos en términos de la confiabilidad de estas técnicas de reconocimiento, siendo necesaria una reflexión general respecto a su compatibilidad con los principios constitucionales y las garantías procesales.

The paper aims to offer an overview of the main features of the biometric discipline and of some problems, emerging from its application in the criminal trial: starting from the necessary terminological clarifications, the biometric method will be presented taking into account the relative accuracy measures that the various systems of recognition may offer in different levels. It will also aim to illustrate the most widespread identification and authentication technologies, including fingerprints, face recognition, iris and retina measurement, voice, gait and genetic testing. Such biometric systems have certain practical advantages not only in private areas (from access to specific places to the use of various services) but also in the criminal trial, in terms of investigations and evidence. After describing the "state of the art" of scientific evidence, particular attention will be devoted to some potentially critical issues, emerging from the relationship between biometric science and the criminal trial. First of all, there is a terminological confusion, deriving from the lack of a single definition, both in literature and in the case-law, of the adjective "biometric". Secondly, to date there are still no unambiguous results in terms of reliability of such recognition techniques and an overall reflection should be started with regard to compatibility with constitutional principles and procedural safeguards.

SOMMARIO

1. Delimitazione del campo d'indagine. – 1.1. Biometria. Precisazioni terminologiche. – 1.2. L'iter biometrico: dal dato biologico grezzo al *template*. – 1.3. Tecniche di identificazione biometrica. – 1.3.1. Le impronte digitali. – 1.3.2. La geometria della mano. – 1.3.3. Il riconoscimento facciale. – 1.3.4. Il riconoscimento dell'iride e della retina. – 1.3.5. Identificazione basata su tratti "dinamici": il riconoscimento vocale e il modo di camminare. – 1.3.6. L'analisi del DNA. – 2. La cornice normativo-giurisprudenziale della prova scientifica: le linee di fondo in materia. – 2.1. Prova scientifica e prova biometrica a confronto. – 3. Conclusioni.

1. Delimitazione del campo d'indagine.

Prima di avviare un'analisi intorno ad alcune questioni connesse all'applicazione della scienza biometrica nel processo penale, si ritiene fondamentale delimitare il campo d'indagine attraverso, in primo luogo, una chiara comprensione del significato del termine "biometria". Tale inquadramento non è facilmente realizzabile, essendo il campo della scienza biometrica assai variegato e complesso¹.

1.1. Biometria. Precisazioni terminologiche.

La biometria (dal greco *βίος*=vita e *μέτρον*= misura) è la disciplina che studia le grandezze biofisiche, sia fisiologiche sia comportamentali, allo scopo di identificarne i meccanismi di funzionamento, di misurarne il valore e di indurre un comportamento desiderato in specifici sistemi tecnologici². Si tratta, dunque, della scienza avente ad oggetto la misurazione delle caratteristiche biologiche tipiche degli organismi viventi, attraverso l'applicazione di alcune tecniche specifiche³. Da un punto di vista tassonomico, in letteratura, con il termine "biometria", si è soliti riferirsi tanto al dato biologico grezzo proveniente da un determinato soggetto, quanto ai particolari sistemi tecnologici che permettono l'identificazione, l'autenticazione o la verifica automatica dell'identità, specie in luoghi o ambiti ove si pongono concrete esigenze di garanzia legate alla sicurezza pubblica o privata⁴. Per tale ragione, non sempre risulta facile, per chi si avvicina allo studio di tale materia, comprenderne la sistematica e la regolamentazione nei vari ordinamenti.

Le caratteristiche biometriche oggetto di misurazione sono generalmente dotate di alcune proprietà essenziali ai fini identificativi e autenticativi tra cui l'"universalità" - il tratto deve essere comune nella popolazione - e l'"unicità", ossia l'elemento in esame deve avere un'alta riferibilità individualizzante⁵.

La prima distinzione da compiere è quella tra caratteristiche biometriche anatomiche o fisiologiche, basate su dati derivanti da misurazioni effettuate su caratteristiche fisiche di una persona, quali l'impronta digitale, l'iride, la retina, la geometria della mano, i tratti somatici del volto⁶ e caratteristiche biometriche comportamentali basate su dati che riguardano aspetti riconducibili a comportamenti propri di un determinato soggetto, quali il riconoscimento vocale, la dinamica di apposizione della firma, l'andatura ecc..

I principali obiettivi che la scienza biometrica si pone, dunque, sono due: in *primis*, verificare la dichiarazione di identità della persona e in secondo luogo, associare l'identità a un

¹ AMATO *et. al.* (2013), p. 10.

² Cfr. "Biometria", Enciclopedie on line - Istituto dell'Enciclopedia italiana Treccani, <http://www.treccani.it/enciclopedia/biometria/> (ultima visualizzazione il 19/2/2019).

³ Cfr. PREITE (2016), p. 21.

⁴ Cfr. PRESIDENZA DEL CONSIGLIO DEI MINISTRI - COMITATO NAZIONALE PER LA BIOETICA (2010), p. 10, http://bioetica.governo.it/media/1846/p95_2010_identificazione-corpo-umano-biometria_it.pdf (ultima visualizzazione il 18/2/2019).

⁵ Altri parametri che generalmente si valutano sono: 1) *invarianza*: la caratteristica deve mantenersi costante nel tempo e indipendente rispetto a qualsiasi variabile; 2) *ammissibilità*: la misurazione deve rispettare l'integrità fisica della persona per poter essere condotta senza metodi troppo invasivi; 3) *acquisibilità*: qualità che consente la rilevazione in modo breve e semplice; 4) *affidabilità*: tale peculiarità deve permettere la ripetizione delle operazioni per verificarne l'esito; 5) *privacy*: riguarda la possibilità di adottare accorgimenti idonei al rispetto della riservatezza; 6) *riducibilità*: consiste nella possibilità di organizzare i risultati e renderli disponibili nelle successive consultazioni; 7) *grado di gradimento*: indica il livello con il quale ogni individuo accetta la metodologia biometrica applicata. Per un approfondimento sul tema tra gli altri cfr. TERRACIANO (2014), pp. 238-239 e WAYMAN *et al.* (2005), p. 2.

⁶ PREITE (2007), p. 43.

soggetto. In caso di accesso “fisico”, il controllo biometrico si realizza attraverso una procedura di accertamento della titolarità personale all’ingresso di una zona o un’area riservata, un edificio protetto, ecc. In caso, invece, di accesso “logico”, il controllo biometrico è effettuato tramite una procedura di accertamento circa la legittimazione della persona interessata (utente) a usufruire di una determinata risorsa informatica. A tal proposito, giova riportare la distinzione fra “verifica”, in cui i dati acquisiti in un determinato momento dal sensore biometrico sono comparati con un unico dato depositato dall’utente nella fase di registrazione e custodito su un dispositivo sicuro o in un archivio magnetico indicizzato (per es. un codice identificativo), e “identificazione”, in cui i dati acquisiti in un determinato momento dal sensore biometrico sono comparati con un insieme di dati contenuti in un archivio o *database*. Pertanto, autenticare significa confrontare un campione biometrico presentato con il corrispondente dato biometrico registrato, relativo ad una singola persona⁷, per accertare che il soggetto sia realmente chi dichiara di essere. I sistemi biometrici di autenticazione/verifica accertano la corrispondenza univoca, effettuando un raffronto di tipo “uno contro uno” tra specifiche caratteristiche fisiche o comportamentali di un individuo stesso, registrato in un *database* o in un dispositivo mobile⁸. L’identificazione è, invece, un vero e proprio processo di attribuzione dell’identità, che si realizza attraverso il raffronto dei dati biometrici di un individuo con tutti quelli memorizzati in un *database*, effettuando un confronto “uno contro molti”. Un sistema può compiere un’identificazione positiva o negativa, dichiarando l’individuo rispettivamente di appartenere o non appartenere al gruppo di utenti noti al sistema.

Nel contesto attuale, i campi di applicazione di tale disciplina risultano i più svariati: dall’accesso a determinati luoghi, al godimento di particolari servizi, alla tracciabilità, con un’evoluzione tecnologica nei campi più differenti (tutela della salute, prevenzione delle frodi sanitarie, protezione dei dati riservati, monitoraggio dell’accesso ad aree riservate, efficienza in attività commerciali, sicurezza nel campo finanziario e militare, controllo alle frontiere e dei flussi migratori etc.)⁹. Il dato proveniente da una precedente autenticazione potrebbe rivelarsi altresì rilevante dal punto di vista penale, per l’accertamento di qualunque elemento utile in ambito investigativo ma anche probatorio¹⁰, eventualmente pure al fine del giudizio di responsabilità.

1.2.

L’iter biometrico: dal dato biologico grezzo al template”

Il metodo di riconoscimento biometrico comincia con la fase di registrazione (*enrollment*), ossia con la rilevazione e l’acquisizione della caratteristica biometrica sotto forma di “dato biometrico grezzo” da parte del sensore cui segue la conversione in un *template*¹¹. Quest’ultimo, detto anche “modello biometrico”, costituisce una rappresentazione matematica digitale del campione biologico. I sistemi di identificazione biometrici archiviano e confrontano per lo più *templates* e non dati biometrici grezzi, i quali vengono principalmente utilizzati per la creazione del *template*.

Una volta terminata la fase di *enrollment*, si apre la procedura di comparazione dei *templa-*

⁷ COUNCIL OF EUROPE, *Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, Progress report on the application of the principle of Convention 108 to the collection and processing of biometric data*, p. 8, «Verification means comparing a presented biometric sample with the corresponding enrolled biometric data pertaining to one single person», <https://rm.coe.int/16806840ba> (ultima visualizzazione il 19/2/2019).

⁸ BISI (2005), pp. 3-35.

⁹ PRESIDENZA DEL CONSIGLIO DEI MINISTRI - COMITATO NAZIONALE PER LA BIOETICA (2010), pp. 4-5, http://bioetica.governo.it/media/1846/p95_2010_identificazione-corpo-umano-biometria_it.pdf (ultima visualizzazione il 18/2/2019).

¹⁰ «Si pensi all’impiego processuale del DNA rinvenuto sul corpo della vittima, quale indizio a carico dell’imputato; al riconoscimento come autentico o meno di un testamento olografo, sulla base dei tratti caratterizzanti la grafia del testatore; alla presenza sulla mano dell’imputato, accusato di aver ucciso taluno con un’arma da fuoco, di tracce di polvere da sparo; alle analisi cliniche e tossicologiche utilizzate per accertare lo stato di salute o le condizioni fisiche dell’imputato o della vittima; alle metodiche di riconoscimento della voce umana in base alla biometria; alle tecniche di pedinamento satellitare; e via discorrendo». GIUNTA (2014), p. 565. Per un approfondimento di veda tra gli altri anche TISTARELLI e CHAMPOD (2017), pp. 5 e ss..

¹¹ NANAVATI *et al.* (2002), p. 17. Si ritiene opportuno specificare che il concetto di *template*, così come quello di campione biologico grezzo risulta centrale per la comprensione e l’analisi delle problematiche relative alla riservatezza piuttosto che alla compatibilità fra le varie tecnologie biometriche e i principi costituzionali posti a garanzia dell’individuo. Infatti, a seconda che il dato venga memorizzato nell’una o nell’altra forma, potrebbe richiedersi una tutela differente, più o meno rafforzata.

tes¹², per determinare il loro grado di somiglianza e di correlazione¹³. Il confronto viene attuato fra il *template* archiviato mediante il processo di *enrollment* (*enrollment template*), e il *template* creato quando l'utente fornisce il proprio dato biometrico al dispositivo di rilevazione del dato stesso (*verification template*). Al livello di somiglianza viene solitamente assegnata una votazione che, in quasi tutti i sistemi, è valutato rispetto a un numero predefinito che funge da limite minimo¹⁴. Se il punteggio eccede la soglia, si verificherà il cd. *match* (combinazione dei *template*) e l'individuo sarà riconosciuto, nel caso opposto la coincidenza non avverrà e il riconoscimento fallirà (*non match*)¹⁵. Dal momento che ogni *template* è unico, le due stringhe di dati, quella archiviata e quella ottenuta "in tempo reale", saranno diverse¹⁶. Per tale ragione, il sensore di cattura deve essere governato da uno specifico algoritmo, il quale consente di confrontare i differenti modelli biometrici per verificarne il grado di coincidenza, che in ogni caso non potrà mai essere totale, e determinare se esso ricade, in base alla valutazione attribuita, al di sopra o al di sotto della soglia considerata accettabile¹⁷. Pertanto, considerato che non è possibile raggiungere un grado di correlazione e somiglianza totale tra i *templates* confrontati, evidentemente la risposta che il sistema biometrico può fornire ai fini del riconoscimento di un soggetto non può che essere, in un certo senso, approssimativa¹⁸.

1.3. *Tecniche di identificazione biometrica*

Il modo migliore per comprendere la portata applicativa della scienza biometrica nel processo penale, ponendo in luce gli aspetti più problematici, è analizzare, seppur per brevi cenni, alcuni dei sistemi d'identificazione più diffusi¹⁹.

1.3.1. *Le impronte digitali*

L'identificazione basata sulle impronte digitali è da considerarsi una delle tecniche maggiormente utilizzate in biometria forense²⁰. Tale sistema sfrutta in modo particolare le tracce

¹² Detta "matching".

¹³ NAVANATI et al. (2002), p. 20.

¹⁴ Tale valore minimo viene generalmente stabilito dall'amministratore del sistema cosicché, a seconda del grado di sicurezza desiderato, è possibile optare per sistemi con soglie più o meno elevate.

¹⁵ È poco probabile che due campioni della stessa caratteristica biometrica, acquisiti in diverse sessioni, coincidano perfettamente (*ut infra*, nota n. 18): questo può verificarsi per molteplici cause, come la presenza di un "rumore", cambiamenti ambientali e la cattiva interazione con l'interfaccia, ossia la superficie del dispositivo attraverso la quale il dato biofisico è acquisito. L'*output* di un sistema di riconoscimento biometrico costituisce un risultato *s* che quantifica la somiglianza fra l'*input* e il *template* archiviato in precedenza nel *database*. Più si rivela elevato il valore del risultato *s*, maggiore sarà la possibilità che i due campioni coincidano. Le principali misure dell'accuratezza di un sistema biometrico sono FNMR, *False Non-Match Rate* e FMR, *False Match Rate*: 1) FNMR si riferisce alla probabilità che due campioni coincidenti, ossia campioni dello stesso tratto biometrico acquisiti dallo stesso utente, siano dichiarati erroneamente come provenienti da due diversi individui (la percentuale si trova anche indicata con la dicitura FRR ossia *False Rejection Rate*); 2) FMR è la probabilità attesa che due campioni appartenenti a due individui diversi siano erroneamente riconosciuti come coincidenti (oppure FAR ossia *False Acceptance Rate*); 3) infine, il parametro FTE (*failure to enroll*) indica la probabilità che un soggetto non sia in grado di essere registrato in un sistema biometrico (altri due parametri, utili ai fini di una comparazione globale dei sistemi, sono EER ossia l'*equal error rate*, che indica il tasso di errore nel punto in cui le curve FAR e FRR si incrociano, e l'*ability to verify* o ATV, che è una combinazione di FTE e FNMR, e indica la percentuale di utenti che saranno in grado di utilizzare il sistema su base giornaliera). La maggior parte dei *False Non-Match Rate* è dovuta a una cattiva interazione dell'utente col sensore del sistema e può essere facilmente risolta permettendo al soggetto di presentare nuovamente l'*input*. L'ipotesi di *False Match Rate*, invece, si riferisce ai tentativi di determinati soggetti che pur non essendone autorizzati, ottengono l'accesso a un sistema, portando a compimento attacchi alla sicurezza dello stesso. Si evince chiaramente che la ricerca del valore di soglia ottimale che permetta un efficace equilibrio fra FMR, FNMR e FTE, rappresenta una delle difficoltà maggiori che incontrano i gestori di sistemi di autenticazione e identificazione basati sulle tecnologie biometriche. Cfr. DELAC e GRCIC (2004), p. 10 e JAIN et al. (2011), p. 328.

¹⁶ Ogni *template* risulta unico e irripetibile in quanto, durante la fase di *enrollment* (*ut supra*, § 1.2), potrebbe subentrare la presenza di numerosi fattori contingenti che variano di importanza a seconda del tipo di dispositivo di rilevazione, come l'illuminazione ambientale, i rumori di sottofondo, il corretto posizionamento dell'utente, il livello di umidità e di temperatura etc.

¹⁷ I sistemi d'identificazione o autenticazione biometrica utilizzano algoritmi proprietari per analizzare i *templates* e generare punteggi. Tali algoritmi trattano i dati contenuti nel *template*, al fine di effettuare un efficace confronto che tenga conto del fatto di cui in nota n. 14. CNIPA, *Linee guida per l'impiego delle tecnologie biometriche nelle pubbliche amministrazioni. Indicazioni operative*, pp.25 e ss., http://www.ordineavvocatitrani.it/upload/linee_guida_tecnologie_biometriche.pdf (ultima visualizzazione il 19/2/2019).

¹⁸ Si veda come esempio di applicazione di quanto detto sopra Cass. pen. Sez. II, (ud. 11-11-2005) 05-12-2005, n. 44358.

¹⁹ Per un approfondimento in materia si veda IOVANE (2008), pp. 181 e ss.

²⁰ Di seguito si riporteranno le tecniche di riconoscimento biometrico più diffuse tralasciando quelle meno utilizzate o poco sfruttate nel contesto forense.

²⁰ Cassazione penale sez. II, 10/10/2018, (ud. 10/10/2018, dep. 25/01/2019), n.3654.

lasciate dalle piccole creste presenti sulle punte delle dita. Ad oggi, attraverso l'utilizzo delle apparecchiature digitali le impronte vengono estratte per mezzo di sensori²¹. Attraverso il metodo cd. *scanning* è possibile realizzare un'immediata registrazione dell'impronta digitale. Ancora più efficiente risulta la cd. "scannerizzazione in diretta", per la quale è anche possibile individuare valori specifici come la temperatura e le pulsazioni del cuore dell'individuo che viene sottoposto all'identificazione. Gli apparecchi digitali consentono, inoltre, di diminuire notevolmente le problematiche connesse alla scarsa definizione dell'immagine dell'impronta (per es. il calore e il sebo epidermico emanato dalle dita della mano). Il sistema di comparazione tra il campione estratto e quello digitale, ottenuto per essere conservato nei *database*, costituisce il principale punto di forza e, contestualmente, la problematica più complessa: i vantaggi si manifestano in termini di accuratezza, velocità e disponibilità immediata di dati ma, da un lato, emergono alcune difficoltà – seppur ad oggi parzialmente superate grazie al progresso scientifico-tecnologico – legate alla necessità che le apparecchiature dispongano di notevoli capacità di calcolo, dall'altro si segnalano le già accennate criticità legate ai falsi positivi²².

1.3.2. *La geometria della mano*

Il sistema di riconoscimento della geometria della mano misura le caratteristiche fisico-geometriche della mano: la forma, la larghezza, la lunghezza delle dita e delle nocche e lo spessore del palmo (o dita). La principale tecnologia impiega una telecamera per catturare alcune misure geometriche comprensive di lunghezze, distanze ed angoli. Nonostante tale sistema, comparso sul mercato intorno agli anni Settanta del secolo scorso²³, sia utilizzato ormai da diversi anni, è ancora piuttosto dibattuto l'aspetto dell'unicità della geometria della mano. Alcuni studiosi sostengono che la geometria della mano non presenti elementi univoci tali da permettere di identificare un individuo come le impronte digitali. Anche dal punto di vista del parametro dell'*invarianza*²⁴, è oggetto di discussione fra gli esperti, poiché possono essere molteplici i cambiamenti nel tempo (per es. per l'età o malattie). Per tale ragione, il sistema considerato viene utilizzato soprattutto per le autenticazioni ossia in modalità "verifica" (cfr. *supra*, § 1.1)²⁵.

1.3.3. *Il riconoscimento facciale*

Il riconoscimento del volto è un sistema innato, utilizzato dagli esseri umani per riconoscersi gli uni con gli altri²⁶. Il sistema biometrico basato sul riconoscimento del viso consiste in un metodo automatico o semi-automatico che registra e paragona le differenze della struttura geometrica del viso, tra cui la forma e la posizione dei suoi attributi – gli occhi, le labbra, il mento – e le loro relazioni spaziali. Durante la rilevazione del dato grezzo, un sensore registra un'immagine o una serie di immagini del volto del soggetto che vengono convertite in formato digitale. Un modello rileva le caratteristiche rilevanti e crea un *template* di dimensioni inferiori rispetto al volto originale rendendo possibile la sua memorizzazione su una *smartcard* o su un passaporto²⁷, utilizzati per i procedimenti di verifica d'identità. Gli strumenti biometrici basati sul riconoscimento facciale sono molto efficienti in quanto sono facilmente "collezionabili" e

²¹ In tempi più risalenti, le impronte venivano estratte premendo la punta di un dito bagnata di inchiostro su di un semplice foglio di carta, in modo tale da lasciare traccia permanente al fine di effettuare gli studi e le comparazioni necessarie.

²² Cfr. *supra*, nota n. 17. Le apparecchiature basate sull'identificazione delle impronte digitali sfruttano due elementi peculiari: le caratteristiche di dettaglio (*local ridges and furrows details* ossia l'analisi dettagliata delle creste e dei solchi dell'impronta digitale) e la configurazione globale (*global pattern configuration*, intesa come la configurazione dell'immagine globale dell'impronta). Relativamente allo studio dei dati raccolti, si è soliti distinguere fra l'approccio statistico (in cui si analizzano i dati oggettivi direttamente dai campi di immagine dell'impronta) e l'approccio strutturale (in cui invece si preferisce analizzare alcuni campioni rilevanti comparando fra loro le specificità). Recentemente, si è individuata una classificazione in riferimento agli algoritmi prima illustrati suddivisa in cinque categorie: arco, arco a tenda, cerchio sinistro, cerchio destro e spirale. Tali elementi vengono ottenuti attraverso la scansione digitale delle impronte, in seguito elaborate, seguendo le peculiarità generali e particolari, per poi analizzarli ai fini di ricerca statistica nei *database*, oppure compararli sulla base della loro struttura.

²³ AMATO *et. al.* (2013), p. 31.

²⁴ Cfr. *supra*, nota n. 6.

²⁵ YORUK *et al.* (2006), pp. 1083-1815.

²⁶ AMATO *et. al.* (2013), p. 33.

²⁷ Tra i 100 e i 3500 byte per i *templates* e tra i 20-40 *kilobytes* per l'immagine originale.

capaci di catturare l'immagine a distanza senza che il soggetto possa accorgersene. Tuttavia, vi sono dei limiti nel sistema: le caratteristiche del volto sono soggette a dei mutamenti (per il trascorrere del tempo, per lesioni, per effetto della chirurgia estetica). La *performance* del sistema può essere influenzata da diversi fattori, quali la distanza del sensore, la visibilità del volto, il grado di cooperazione del soggetto e la qualità delle immagini²⁸.

1.3.4. *Il riconoscimento dell'iride e della retina*

I sistemi biometrici basati sulla struttura dell'iride sono in grado di identificare, in tempo reale, l'individuo attraverso la misurazione dell'iride²⁹. Il soggetto guarda verso il sensore permettendo l'illuminazione della struttura dell'iride da parte di un laser a bassa intensità, una luce infrarossa che effettua la scansione dell'occhio e consente di rilevare le sue particolarità. Un algoritmo rappresenta in termini matematici la struttura dell'iride. I limiti dei sistemi di identificazione basati sul riconoscimento dell'iride sono legati al fatto che è necessario posizionare opportunamente l'occhio: il processo di localizzazione costituisce un importante passaggio, poiché, se eseguito scorrettamente, può comportare una contaminazione da parte di eventuali disturbi esterni in corso di riconoscimento (per es. i riflessi), oppure nei pressi dello stesso bulbo oculare (quali le ciglia e le pupille). Dal punto di vista del parametro dell'“invarianza”³⁰, l'iride – a parte i primi mesi di vita – rimane pressoché immutata durante il corso della vita dell'individuo. Tale tecnica viene utilizzata soprattutto nell'ambito della sicurezza e non è considerata invasiva poiché non vi è alcun contatto fisico fra il soggetto e lo strumento di rilevazione.

Considerando, invece, il riconoscimento biometrico della retina (ad oggi, tecnica molto poco utilizzata), il principale aspetto caratterizzante è costituito dallo studio del sistema vascolare. Sebbene tale tecnologia venga considerata un'efficiente sistema di identificazione personale, essa risulta di difficile impiego e piuttosto invasiva³¹.

1.3.5. *Identificazione basata su tratti “dinamici”: il riconoscimento vocale e il modo di camminare.*

I sistemi biometrici basati sul riconoscimento vocale funzionano attraverso la misurazione della voce, componente comportamentale dell'individuo risultante dalle caratteristiche fisiche specifiche di ciascun individuo come la forma e la grandezza dei tratti vocali, del mento, delle cavità nasali, delle labbra³². Tali sistemi di identificazione sono utilizzati anche per i processi di verifica/autenticazione e hanno avuto recente diffusione in settori come la finanza (*e-commerce* e *e-banking*) e nell'ambito forense (la polizia giudiziaria registra la voce per poi eseguire il *matching* con la conversazione telefonica intercettata ai fini dell'indagine e se il confronto dà esito positivo, quest'ultimo può essere successivamente utilizzato come prova durante il processo³³). La voce è da sempre considerata un parametro universale con un certo grado di “permanenza” (può modificarsi a seconda dell'età, dello stato emotivo o dello stato di salute) ed è di facile “collezionabilità”³⁴.

Per quanto concerne i sistemi biometrici basati sull'andatura del soggetto, essi funzionano a partire da una telecamera che cattura la specifica modalità in cui un soggetto cammina mi-

²⁸ Per un approfondimento si veda MASTRONARDI (2014), pp. 1-12; Cassazione penale sez. I, 03/12/2018, (ud. 03/12/2018, dep. 14/01/2019), n.1524.

²⁹ AMATO *et al.* (2013) p. 35. Per un approfondimento sul tema si veda anche LA REGINA (2018), p. 212.

³⁰ Cfr. *supra*, nota n. 6.

³¹ La tecnica necessita di un contatto fra il sensore e l'occhio del soggetto: nella maggior parte dei casi, tale sistema di identificazione è percepito dagli utenti come pericoloso.

³² Cfr. GRIMALDI *et al.* (2014), p. 2014. Le tecnologie legate a tale dato biometrico possono essere di due tipologie: il *text dependent* e il *text independent*. Nel primo, il soggetto da identificare pronuncia una frase che, tradotta in *template*, viene codificata in un algoritmo. Nel secondo, la voce del soggetto è riconosciuta a prescindere da ciò che sta parlando: le onde sonore emesse dall'individuo sono registrate e calcolate come vettori caratteristici che vengono assunti da modello (*template*) dell'individuo. Durante la fase di riconoscimento, le sequenze dei vettori vengono comparate usando il campione.

³³ AMATO *et al.* (2013), p. 37.

³⁴ Cfr. *supra*, nota n. 6.

surando la forma e/o le dinamiche del corpo, l'andatura delle gambe, la cadenza e la velocità del passo³⁵. L'andatura non è considerata una caratteristica "universale" ma è comunque un elemento identificativo. Dal punto di vista della "permanenza", esso può variare a seconda della muscolatura, con il trascorrere del tempo, durante la gravidanza, a causa di lesioni o in condizioni alterate dell'individuo (per es. in stato d'ebbrezza).

1.3.6. *L'analisi del DNA.*

Ciascun essere umano è identificabile attraverso il proprio codice genetico del DNA: esso si può definire come una lunga molecola presente all'interno delle nostre cellule, nella quale si raccoglie un enorme quantità di informazioni necessarie per lo sviluppo dell'individuo, per la costruzione di ampie varietà di strutture biologiche e per il mantenimento dei processi vitali³⁶. Alla base del lavoro dei genetisti forensi vi è l'acquisizione delle sezioni di tali molecole al fine di descriverne le singole caratteristiche genotipiche³⁷.

La profilazione del DNA in ambito forense è ormai un mezzo di prova generalmente accettato da parte delle autorità giurisdizionali, tanto da aver portato alla costituzione di *database* specifici in un'ottica di cooperazione internazionale, per fini legati all'identificazione personale e alla sicurezza.

Tutte le cellule dotate di un nucleo contengono frammenti di DNA identico per un medesimo individuo e perciò la maggior parte dei materiali biologici lasciati dal nostro corpo consentono di risalire all'identità personale³⁸. Solitamente in ambito forense vengono comparati due profili di DNA: uno rilevato sul luogo del delitto ed un altro di riferimento, estratto da un sospetto criminale. Nessun problema si pone se i due profili risultano essere differenti mentre, se i due profili corrispondono, allora sarà necessario comprendere se il campione di DNA ricavato dalla *scena criminis* appartiene realmente al sospettato o a qualcun altro avente lo stesso profilo genetico (la probabilità che ciò si verifichi è pari a 1 su un miliardo)³⁹. Vi sono poi numerosi altri fattori che possono elevare la possibilità che si tratti di un errore di falsa corrispondenza: il campione biologico grezzo potrebbe contenere solo una minima quantità di DNA o il profilo rilevato sul luogo del delitto potrebbe essere stato danneggiato o contaminato. L'evoluzione tecnologica e digitale ha consentito un notevole miglioramento degli studi scientifici e delle tecniche di analisi dei campioni di DNA e il diritto ha tentato negli anni di disciplinare l'utilizzo di tali tecniche⁴⁰.

2. *La cornice normativo-giurisprudenziale della prova scientifica: le linee di fondo in materia.*

Con l'espressione "prova scientifica" s'intende correntemente qualsivoglia accertamento che produca un risultato utile per il processo e che richieda per il suo espletamento il ricorso

³⁵ Alla base del funzionamento di tale tecnica vi è l'utilizzo di un algoritmo per la determinazione delle relazioni matematiche intercorrenti fra ogni punto del corpo in movimento ed il *template* necessario al fine del riconoscimento. Si veda Ass. App., Torino, n. 21/15 Reg. Sent., 22.02.2016; Cassazione penale sez. I, 03/12/2018, (ud. 03/12/2018, dep. 14/01/2019), n.1524; Cassazione penale sez. I, 08/06/2018, (ud. 08/06/2018, dep. 13/09/2018), n. 40722.

³⁶ L'analisi del DNA è stata recentemente ammessa tra le tecnologie biometriche che sono all'attenzione del sub-comitato di standardizzazione ISO (ISO/IEC JTC1 SC 37 "*Biometrics*") anche se, a differenza di quanto avviene per tutte le altre tecnologie biometriche, almeno per il momento l'analisi del DNA non permette un'autenticazione in tempo reale. Quest'ultimo criterio non è tuttavia contemplato nella canonica definizione di tecnologie biometriche e quindi non impedisce di annoverare l'analisi del DNA tra di esse.

³⁷ In tempi più risalenti veniva utilizzato il metodo *fingerprint*, in cui il profilo genetico era raffigurato con una sezione di grafico a barre. Successivamente, grazie al metodo *Mullis* e la cd. "reazione a catena della polimerasi", il profilo genetico veniva descritto con una semplice sequenza di numeri: il frammento del DNA studiato viene riprodotto diversi milioni di volte, in modo da poterlo analizzare a livello macroscopico. Cfr. "*Fingerprinting*", Enciclopedie on line - Istituto dell'Enciclopedia italiana Treccani, [http://www.treccani.it/enciclopedia/fingerprinting_\(Dizionario-di-Medicina\)/](http://www.treccani.it/enciclopedia/fingerprinting_(Dizionario-di-Medicina)/) (ultima visualizzazione 19/2/2019).

³⁸ Dal punto di vista della preparazione dei campioni e delle modalità di analisi, si ritiene come i marcatori del DNA siano collocati generalmente in una regione non codificata dei cromosomi cellulari. Il genoma umano è costituito da sequenze ripetute di DNA: le cd. STRs - *short tandem repeat* - sono individuate intorno alla struttura dei cromosomi nella zona strutturale centrale, componenti fondamentali per l'identificazione degli esseri umani. Cfr. MASTRANGELO (2017), GALGANI (2006), p. 40, RICCI (2001), pp. 108 e ss.

³⁹ AMATO *et. al.* (2013), p. 39.

⁴⁰ Per un approfondimento si vedano tra gli altri RICCI (2018), p. 93; RIVELLO (2016), pp. 1521-1531; UBERTIS (2016), pp. 1198 e ss.; RENZETTI (2015), pp. 399 e ss.; BARGIS (2011), pp. 49 e ss. CAPRIOLI (2008), pp. 3523; FERRUA (2008), pp. 12 e ss.; PULITANÒ (2006), p. 802.

a conoscenze tecnico-scientifiche⁴¹. L'utilizzo di leggi scientifiche per ricostruire i fatti da cui dipende la decisione sulla *res iudicanda* non trova nel diritto processuale una sua specifica regolamentazione. Il codice di rito penale prevede uno specifico mezzo di prova – la perizia – destinato ad essere ammesso «quando occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche o artistiche» (art. 220, comma 1 c.p.p.). Laddove debbano essere adottate competenze del suddetto genere – e ricorrono le condizioni per l'ammissibilità d'ogni mezzo istruttorio, oltre a quella, peculiare, integrata dalla occorrenza dell'intervento da parte del “testimone esperto” – il disporre la perizia costituisce per il giudice un vero e proprio obbligo⁴². Tuttavia, secondo il vigente ordinamento processuale penale, l'espletamento della tipica attività istruttorio prevista dagli artt. 220 ss. c.p.p. non è l'esclusivo veicolo per l'ingresso in sede giudiziaria del sapere tecnico-scientifico: il modello conosce altresì l'istituto della consulenza tecnica di parte esperibile «fuori dai casi di perizia» (art. 233 c.p.p.). Ciascuna delle parti è pertanto legittimata a designare fino a due propri esperti, per essere da questi assistita, nelle questioni implicanti «specifiche competenze tecniche, scientifiche o artistiche», fin dalle indagini preliminari (artt. 359, 360, 391-bis ss. c.p.p.)⁴³.

Comè noto, negli Stati Uniti alcune delle questioni più rilevanti connesse all'uso della prova scientifica sono state affrontate non solo a livello legislativo, ma anche giurisprudenziale⁴⁴. I pilastri dell'orientamento giurisprudenziale statunitense in materia sono costituiti dai due *leading cases*. Innanzitutto il caso *Frye vs. United States*⁴⁵, deciso dalla Corte d'appello del distretto di Columbia e, in secondo luogo, la decisione *Daubert vs. Merrel Dow Pharmaceuticals*⁴⁶, disposta nel 1993 dalla Suprema Corte Federale. Inoltre, si segnalano le *Federal rules of evidence* del 1975 (in particolare le *rules* 702 e 703) aventi ad oggetto la *testimony by experts*. In particolare, la *Circuit Court del District of Columbia*, nel caso *Frye* del 1923, avente ad oggetto l'ammissibilità come prova dei risultati sperimentali dell'utilizzazione di un poligrafo (una primordiale “macchina della verità”), aveva indicato come parametro di valutazione dell'attendibilità della prova scientifica, quello del consenso della comunità scientifica di riferimento (cd. *general acceptance test*), così dichiarando inammissibile la richiesta istruttorio avanzata dalla difesa⁴⁷. Tuttavia, tale criterio interpretativo non tardò a manifestare i suoi limiti, non solo perché in tal modo la prova scientifica “nuova”, in quanto priva di un giudizio di *general acceptance*, avrebbe potuto essere ammessa – a prescindere dalla sua validità – ma anche e soprattutto per l'evidente ragione che il consenso della comunità scientifica non avrebbe potuto attribuire di per sé ad una tecnica di indagine l'idoneità a dimostrare i fatti oggetto di accertamento.

Successivamente, la *Federal Supreme Court* degli USA, nella sentenza del 28 giugno 1993 relativa al caso *Daubert*, fu investita del problema dell'ammissibilità di una prova scientifica fondata su principi che non apparivano sufficientemente consolidati da ricevere generale accoglienza nella comunità scientifica nello specifico campo di ricerca. La Corte ha indicato alcuni criteri per valutare l'ammissibilità delle prove scientifiche (e dunque a dare ingresso processuale anche alla cd. “scienza nuova”) e, in sostanza a verificarne la validità e attendibilità. Il primo criterio elaborato dalla *Supreme Court* è quello della verificabilità ossia della falsificabilità della tecnica a fondamento della prova; il secondo criterio è rappresentato dalla sottoposizione della teoria o tecnica al controllo, alla revisione critica da parte degli altri membri della comunità scientifica (*peer review*) nonché dalla pubblicazione dei risultati delle relative ricerche su riviste specializzate (*publication*); il terzo (duplice) criterio richiede che il giudice, nel vagliare l'ammissibilità della prova scientifica, tenga conto della frequenza (o percentuale) di errore, conosciuta o potenziale, nonché della presenza di standard costanti di verifica, ossia dell'eventuale riscontro di una molteplicità di casi; ai menzionati criteri si deve poi naturalmente aggiungere quello del consenso generale da parte della comunità scientifica che, se non deve essere utilizzato quale strumento esclusivo di valutazione per l'ammissione della *expert*

⁴¹ In particolare, O. Dominioni ha affermato che la prova scientifica «(...) è una espressione ellittica che designa un complesso fenomeno (...) si tratta di operazioni probatorie per le quali, nei momenti dell'ammissione, dell'assunzione e della valutazione, si usano strumenti di conoscenza attinti alla scienza ed alla tecnica». DOMINIONI, (2005), p. 12. Per un approfondimento sulla prova scientifica si veda anche TONINI (2010b), p. 321.

⁴² LORUSSO (2008), pp. 295 e ss.

⁴³ FORTE (2018), p. 2267.

⁴⁴ Per un approfondimento si vedano tra gli altri KAUFMAN (2001): pp. 7-20; GRAHAM (2000): pp. 322 e ss.; BAROVICK (1999), p. 1533; GRAHAM (1992), p. 243.

⁴⁵ *Frye v. United States*, 293 F. 1013 (D.C. Cir., 1923).

⁴⁶ *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).

⁴⁷ Ossia quella di ammettere come prova nel processo la sottoposizione dell'imputato al test della macchina della verità.

scientific testimony, può comunque offrire conferme importanti in ordine alla validità di una teoria o tecnica scientifica che si intenda utilizzare nel processo. Il giudice, nell'analizzare tali prove, deve assumere il ruolo di "guardiano" ("*gatekeeper*"), cui è assegnato il compito di valutare l'affidabilità e la validità dei *methods and procedures* che presiedono alla formazione di ogni singola prova scientifica che le parti intendono dedurre nel processo.

I criteri individuati nel caso *Daubert* costituiscono, come riconosciuto dalla stessa Corte Suprema USA, massime o regole di esperienza, certamente idonee per le finalità perseguite, ma non definitivamente risolutive. Ad esse possono dunque ragionevolmente affiancarsi anche quelle che giurisprudenza e dottrina hanno ulteriormente proposto o vorranno proporre, naturalmente senza pretendere che i diversi criteri elaborati debbano ogni volta coesistere tra loro. Com'è noto, la nostra giurisprudenza di legittimità si è occupata di temi connessi alla valutazione di affidabilità della prova scientifica ma ha più volte dimostrato di riconoscere validità ai criteri elaborati dalla giurisprudenza statunitense⁴⁸.

Se il codice di procedura penale italiano odierno "contiene" in sé norme specifiche concernenti sia il momento dell'ammissione sia quello dell'acquisizione della perizia, non altrettanto si può affermare per quanto concerne la terza fase del procedimento probatorio: quello di valutazione dei corrispondenti risultati. L'articolo 192 c.p.p. dispone che «il giudice valuta la prova dando conto nella motivazione dei risultati acquisiti e dei criteri adottati». Domina, pertanto, l'idea per cui il giudice possa liberamente valutare gli esiti di quei procedimenti probatori che siano stati ammessi ed acquisiti legittimamente⁴⁹, purché siano adeguatamente motivati in sentenza quei risultati che ha ritenuto determinanti ai fini della decisione assunta, nonché delle massime d'esperienza impiegate nell'apprezzarli. Perciò, il giudice, obbligato a disporre la perizia – poiché imposta dall'esigenza di specifiche competenze scientifiche –, una volta che la perizia stessa sia stata eseguita, non è tenuto a decidere conformemente ai risultati della corrispondente procedura acquisitiva, fermo restando, però, l'obbligo di un'adeguata motivazione nella statuizione circa il suo diverso avviso⁵⁰. A tal proposito, il giudice diviene *peritus peritorum*, il quale pur dovendo avvalersi di esperti, non è vincolato alle loro conclusioni e può disattenderle. Il magistrato, in ogni caso, deve essere in grado di "controllare" l'esperimento della prova scientifica, comprendere la "sintassi" del ragionamento e il percorso seguito dall'esperto per giungere alle sue conclusioni⁵¹; egli deve essere inoltre in grado di conoscere i limiti scientifici della prova, in modo da divenire fruitore consapevole della scienza che viene introdotta nel processo⁵²: deve assumere cioè quel ruolo che la giurisprudenza americana ha definito di "*gatekeeper*"⁵³.

⁴⁸ Cass. Sez. 1, Sentenza n. 31456 del 21 maggio 2008 (dep. 29 luglio 2008) Rv. 240764, Franzoni, in tema di applicazione della *Bloodstain Pattern Analysis* - tipo di indagine che studia la morfologia e disposizione delle macchie ematiche rinvenute sugli oggetti presenti sul luogo del delitto, per verificare la provenienza dei colpi inferti alla vittima e la reciproca posizione di quest'ultima e dell'aggressore - la Corte ha evidenziato come nel caso specifico fossero stati rispettati «anche i rigorosi criteri di validazione della prova scientifica (aventi per l'A.G. italiana natura meramente orientativa) elaborati dalla giurisprudenza degli USA» (per un approfondimento cfr. CAPRIOLI (2009), pp. 1867 e ss.); Cass., Sez. 4, Sentenza n. 43786 del 17 settembre 2010 (dep. 13 dicembre 2010) Rv. 248943 Cozzini, la quale ha intrapreso una vera e propria opera di ricostruzione dei criteri che il giudice di merito deve seguire nella valutazione della validità della prova scientifica, ispirandosi - pur senza farvi esplicito riferimento - alle linee guida dettate dalla giurisprudenza statunitense, ritenute questa volta non più solo meramente orientative ma del tutto vincolanti; Cass. Sez. 5, Sentenza n. 36080 del 27.03.2015 (dep. 7.09.2015), Knox, in motivazione (p. 35): «(...) un risultato di prova scientifica può essere ritenuto attendibile solo ove sia controllato dal giudice, quantomeno con riferimento all'attendibilità soggettiva di chi lo sostenga, alla scientificità del metodo adoperato, al margine di errore più o meno accettabile ed all'obiettiva valenza ed attendibilità del risultato conseguito». Ancora, secondo Cass. Sez. 2, Sentenza n. 12751 del 08/03/2011 Ud. (dep. 29/03/2011) Rv. 250049, Cutaia, le nuove metodologie su cui si fonda la "prova nuova" quale presupposto per la richiesta di revisione, devono essere «accreditate e ritenute pienamente attendibili dalla comunità scientifica». Inoltre, secondo Cass. N. 3031 del 22.10.2009, Allegro, l'accertamento peritale proposto con la richiesta di revisione, ove richieda il ricorso a «nuove tecniche e a nuove conoscenze», deve porsi come «il risultato di protocolli di indagine riconosciuti dalla comunità scientifica». Analogamente Cass. Sez. 6, Sentenza n. 34531 del 04/07/2013 Ud. (dep. 08/08/2013), Mazzagatti, in motivazione: «(...) deve ovviamente trattarsi di applicazioni tecniche accreditate e rese pienamente attendibili dal livello del sapere acquisito dalla comunità scientifica, dato che soltanto tale condizione conferisce un tasso di ragionevole affidabilità ai risultati della nuova indagine».

⁴⁹ Cfr. CORDERO, (2012), p. 569; CECCHI (2017), pp. 915 e ss.; TONINI (2015), pp. 1410 e ss..

⁵⁰ In tal senso, TONINI, (2011), p. 364; inoltre, si veda Cass., Sez. IV, 13 dicembre 2010, n. 43785 in Guida Dir., 2011, n. 6 secondo la quale «quando il sapere scientifico non è consolidato o non è comunemente accettato perché vi sono tesi in irrisolto conflitto, spetta comunque al giudice prescegliere quella da preferire».

⁵¹ TARUFFO (2005), p. 1079: «(...) è necessario che il giudice sia in grado almeno di valutare la validità dei metodi di cui il consulente si è servito per svolgere il suo compito».

⁵² Giova segnalare quanto affermato da O. Dominioni «non è consentito che nella funzione probatoria si usino apparati conoscitivi insuscettibili di controllo ad opera del giudice e delle parti», DOMINIONI (2005), p. 69.

⁵³ Come osservato da Cass. 36080/2015, Knox, cit., in motivazione (p.33): «La conseguenza dell'ineludibile presa d'atto di tale stato di legittima ignoranza del giudice, e dunque della sua incapacità di governare "autonomamente" la prova scientifica, non può, però, essere l'acritico affidamento, che equivarrebbe - anche per un malinteso senso del libero convincimento e di altrettanto malinteso concetto di "perito

2.1. *Prova scientifica e prova biometrica a confronto.*

Diverse sono le problematiche che emergono in seno al rapporto fra prova scientifica e prova biometrica. La prima affonda le sue radici da una previa questione terminologica che riguarderebbe l'uso alternativo dell'aggettivo "biometrico" sia per quel che concerne il dato biologico grezzo sia per il cd. *template*⁵⁴ (cfr. *supra*, § 1). La confusione nascerebbe da un uso sinonimico dell'aggettivo "biometrico" in riferimento al campione biologico rilevato per esempio sulla *scena criminis* e il dato contenuto all'interno del supporto digitale o ancora in relazione all'algoritmo utilizzato per il funzionamento del sistema di riconoscimento⁵⁵. In ogni caso, sia ci si riferisca al campione biologico grezzo, sia si consideri il *template*, si ritiene che la prova biometrica costituisca una *species* del più ampio *genus* di "prova scientifica"⁵⁶. A seconda, poi, della tipologia di tecnologia che viene utilizzata all'interno del processo penale (più o meno avanzata) si potrà operare un distinguo fra "prova scientifica" e "prova scientifica nuova"⁵⁷.

In secondo luogo, la biometria applicata al contesto forense ha fatto emergere dubbi riguardanti l'assoluta affidabilità dei risultati scaturenti dall'applicazione dei sistemi di identificazione⁵⁸. Parte della dottrina ha sostenuto l'alto grado di attendibilità, ritenuto prossimo alla certezza e la compatibilità con gli standard "Daubertiani" probatori richiesti in tale sede (cfr. *supra*, § 2.1), dei metodi scientifici ad esse sottesi e della controllabilità oggettiva delle modalità di formazione del dato cognitivo. Dall'altra parte, un margine di errore nei sistemi di identificazione o autenticazione, come per qualsiasi sistema statistico di comparazione, risulta pur sempre presente e come tale è suscettibile di creare problematiche in ambito processuale⁵⁹. I cambiamenti delle condizioni ambientali e di registrazione e acquisizione dei dati, così come i cambiamenti fisici (temporanei o permanenti) o il tempo intercorrente tra l'*enrollment* e la comparazione biometrica, giocano un ruolo fondamentale, riducendo le possibilità di riconoscimento. Peraltro, la disciplina biometrica si basa tipicamente su leggi di tipo statistico che consentono di elaborare previsioni sull'incertezza del risultato, ma non di accertare i fatti: è noto il dibattito relativo ai rapporti tra scienze statistiche e accertamento penale⁶⁰.

Oltre a ciò, si ritiene che in tutti i casi in cui le tecniche di identificazione biometriche richiedano il prelievo di materiale biologico grezzo dalla persona sottoposta alle indagini o, a fortiori, di terzi al procedimento, si pongano problematiche relative alla compatibilità coi principi costituzionali eretti a tutela dei diritti fondamentali dell'uomo⁶¹ (il diritto alla dignità, alla libertà personale, alla salute e, secondo parte della dottrina, il diritto di difesa)⁶². Si aggiunga altresì il rischio intrinseco legato all'adozione di tali metodi di indagine in relazione all'oggetto su cui vertono, di cagionare una lesione al diritto alla riservatezza dei dati personali⁶³, considerato nella duplice componente positiva ad esercitare una verifica sulla correttezza e sulla circolazione dei dati e in quella negativa riguardante il diritto di escludere dalla fruizione del dato tutti i soggetti che ne sono titolari⁶⁴.

Si può, inoltre, sostenere che sia ravvisabile un problema di compatibilità del procedimento tecnico-scientifico volto all'analisi e alla comparazione dei dati con le fasi in cui si articola solitamente il processo penale, e, in particolare, un problema di inquadramento delle singole

dei periti" - a sostanziale rinuncia al proprio ruolo, mediante fideistica accettazione del contributo peritale, cui delegare la soluzione del giudizio e, dunque, la responsabilità della decisione». Per un approfondimento sul ruolo del giudice tra gli altri cfr. BARTOLI (2018), p. 12.

⁵⁴ Cfr. *supra*, § 1.2.

⁵⁵ Cfr. PRESIDENZA DEL CONSIGLIO DEI MINISTRI - COMITATO NAZIONALE PER LA BIOETICA (2010), p. 6, http://bioetica.governo.it/media/1846/p95_2010_identificazione-corpo-umano-biometria_it.pdf (ultima visualizzazione il 28/2/2019).

⁵⁶ Il *template* inteso come dato biologico contenuto in un supporto digitale è considerato non solo "prova biometrica" ma anche "digitale" definita dallo *Scientific Working Group on Digital Evidence* come qualsiasi informazione con valore probatorio, che sia o meno memorizzata o trasmessa in un formato digitale (cfr. <https://www.swgde.org/> - ultima visualizzazione il 19/2/2019). Per un approfondimento si veda DANIELE (2011), pp. 297 ss.

⁵⁷ DOMINIONI (2005), pp. 83 e ss.

⁵⁸ FANUELE (2009), pp. 1-2.

⁵⁹ Ad esempio, gli errori compiuti da un sistema per il riconoscimento del volto sono generalmente maggiori di quelli riscontrabili in sistemi basati sul riconoscimento delle impronte digitali o dell'iride.

⁶⁰ Per un approfondimento si veda tra gli altri BLAIOTTA (2010).

⁶¹ Emerge l'esigenza di un bilanciamento delle esigenze connesse all'accertamento dei reati con la tutela dei diritti di rango costituzionale, come il diritto alla dignità personale, alla libertà, alla salute e alla riservatezza. Cfr. FANUELE (2009), p. 38; FELICIONI (2007), p. 16; KOSTORIS (2006), p. 330.

⁶² Per una riflessione volta ad individuare le possibili ricadute tra indagine genetica e garanzia del diritto di difesa, FELICIONI (2007), p. 26 e GIUNTA (2014), p. 568.

⁶³ SELLAROLI (2006), p. 71.

⁶⁴ Cfr. tra gli altri QUATTROCOLO (2019), pp. 2 e ss.; ALLEGREZZA (2007), p. 65; BONETTI (2003), p. 11.

attività scientifiche preposto alla formazione del dato cognitivo all'interno della cornice dei mezzi di prova catalogati all'interno del codice del 1988. Un esempio paradigmatico delle difficoltà che si pongono al giurista interprete nell'opera di armonizzazione delle tecniche di identificazione biometrica con i paradigmi del processo penale è rappresentato dalla disciplina della dattiloscopia⁶⁵. Tale metodo di riconoscimento si snoda in due fasi principali: la prima volta al rilevamento dell'impronta digitale mediante l'impiego di tecniche che si differenziano in ragione della morfologia della traccia rinvenuta, mentre la seconda fase è preordinata alla comparazione dell'impronta rinvenuta in sede di rilievi sulla *scena criminis* con quella prelevata dalla persona sottoposta alle indagini⁶⁶. Inquadrando l'attività tecnico-scientifica nella cornice processuale, ferma la previsione dell'articolo 349 comma 2 c.p.p., che menziona gli accertamenti dattiloscopici della polizia giudiziaria in sede identificativa, si segnala un contrasto interpretativo. Da un lato, la giurisprudenza tende a ricondurre entrambe le fasi di rilevazione e comparazione delle impronte all'interno dell'articolo 354 commi 2 e 3 c.p.p., in forza del loro carattere meramente materiale. Dall'altra, parte della dottrina propone una distinzione tra le due fasi, qualificando il *matching* come un'attività di carattere valutativo da espletarsi nelle forme della consulenza (*ex art. 360 c.p.p.*) o nelle forme della perizia. La risoluzione della questione non può di certo prescindere dalla correttezza della summenzionata distinzione fra operazione di carattere materiale (riferibili alla nozione di "rilievo") e le attività di carattere valutativo inquadrabili nell'espressione codicistica di "accertamento tecnico". Va inoltre osservato che il distinguo prospettato non permette l'applicazione in ogni caso del corredo di garanzie difensive fornite dall'articolo 360 c.p.p. la cui operatività va circoscritta agli accertamenti tecnici (e non ai rilievi materiali) non procrastinabili al dibattimento per cause relative alla deteriorabilità dell'oggetto di indagine in seguito alle attività di analisi⁶⁷. Dunque, nel caso in cui si vogliano acquisire tali elementi di prova nel processo affinché il giudice possa valutarli, occorrerà procedere con le forme della consulenza e della perizia che garantiscono la salvaguardia del principio del contraddittorio nonché la controllabilità del metodo prescelto con riguardo alla morfologia dell'impronta rinvenuta e del rispetto dei criteri valutativi relativi all'attività di *matching*⁶⁸.

3. Conclusioni

Con il presente contributo si è cercato di presentare e descrivere i principali caratteri della disciplina tecnico-scientifica denominata "biometria" che ha come scopo quello di automatizzare le procedure di identificazione o di verifica dell'identità, attraverso la valutazione di caratteristiche fisiche e/o comportamentali degli esseri umani, acquisite da sensori elettronici, elaborate da specifici algoritmi matematici e, infine, trasformate in modelli matematici. La scienza biometrica, come altre, non è priva di errori, a maggior ragione se si considera la sua natura tipicamente statistico-probabilistica. L'introduzione sistematica di tecnologie biometriche all'interno del processo penale, potrebbe, pertanto, comportare alcune problematiche in termini di affidabilità dei risultati scaturenti dalla loro applicazione e di compatibilità fra la disciplina in esame, i principi costituzionali e le tipiche garanzie processuali. Tuttavia, a seguito del notevole sviluppo tecnologico recente, il processo penale pare non poter più fare a meno dei contributi offerti dalla biometria, soprattutto perché sia la scienza sia il processo, anche se con diversi approcci, hanno il comune obiettivo della ricostruzione del nesso causale. I dati biometrici devono essere analizzati e valutati in termini di "accuratezza scientifica" e si deve caso per caso comprendere quale tipo di "valore" accordare loro.

I rischi più determinanti in capo alla scienza forense nella sua recente dimensione digitale e nei suoi approfondimenti di studio sulla biometria, stanno a poco a poco trasformando il

⁶⁵ Non è, infatti, possibile dar conto, in questa sede, di tutti i limiti relativi ai metodi di identificazione riportati nei paragrafi precedenti né della parabola evolutiva percorsa dalla tecnologia in riferimento ai singoli sistemi di riconoscimento.

⁶⁶ La giurisprudenza richiede che vi siano almeno diciassette punti di coincidenza affinché il risultato identificativo sia utilizzabile in sede penale.

⁶⁷ Sulla nozione di irripetibilità si vedano CESARI (1999), p. 8 e ICHINO (1992), p. 45.

⁶⁸ Si ritiene che la medesima interpretazione pare ispirare altresì la disciplina di un'altra prova biometrica, quella del DNA, inquadrabile nella cornice della consulenza tecnica e della perizia. L'inquadramento di tale mezzo di prova è reso complesso, da un lato, dalla varietà delle tecniche di analisi dei vari profili genetici e, dall'altro, dall'attitudine della disciplina a comprimere diritti di rilevanza costituzionale. Per un approfondimento sulla prova genetica si veda FANUELE (2009), pp. 95 e ss., FELICIONI (2009), pp. 6-24.

sistema attuale della giustizia penale. In questo senso, è auspicabile un intervento legislativo chiarificatore teso a uniformare la disciplina e che distingua un dato biometrico da un altro, e le differenti applicazioni che possono essere messe in atto, dal momento che la specificità di ciascun dato e degli ambiti di impiego impone soluzioni giuridiche differenziate. Altrimenti, il pericolo è quello dell'affievolirsi notevolmente delle garanzie processuali (come per esempio il principio del contraddittorio, quello della ragionevole durata del processo nonché del diritto alla difesa) oltre ad alcune problematiche legate a più ampie garanzie individuali come il diritto alla riservatezza. Peraltro, uno degli obiettivi principali del Garante privacy è quello di limitare l'utilizzo di tali tipologie di dati attraverso il ricorso a mezzi alternativi di autenticazione e identificazione meno invasivi della sfera personale e della libertà individuale, sussistendo un'inderogabile esigenza di rispettare il corpo umano, salvo sia strettamente necessario e conforme al principio di proporzionalità, procedere diversamente⁶⁹.

A conclusione di queste brevi riflessioni suonano quanto mai profetiche le parole di Stefano Rodotà al proposito: «L'unità della persona può essere ricostruita solo estendendo al corpo elettronico il sistema di garanzie costruito per il corpo fisico»⁷⁰.

Bibliografia

ALLEGREZZA, Silvia (2007): "Giustizia penale e diritto all'autodeterminazione dei dati personali nella regione Europa", in NEGRI Daniel (eds.): *Protezione dei dati personali e accertamento penale* (Roma, Aracne editore), pp. 59-85

AMATO Salvatore, CRISTOFARI Fabiana, RACITI Salvatore (2013): *Biometria. I codici a barre del corpo* (Torino, Giappichelli)

BALOSSINO Nello e SIRACUSA Simona (2004): *L'identificazione basata sul volto: metodi fisiologici e metrici* (Milano, Itasforum)

BARGIS, Marta (2011): "Note in tema di prova scientifica nel processo penale", *Rivista di diritto processuale*, 66 (1), pp. 49 – 66

BAROVICK Robin (1999): "Between Rock and Hard Place: Polygraph Prejudice Persist After Scheffer", *Buffalo Law Review*, 47, pp. 1533 e ss.

BARTOLI, Roberto (2018): "Diritto penale e prova scientifica" in CANZIO Giovanni e LUPARIA Luca (eds.), *Prova scientifica e processo penale* (Milano, Wolters Kluwer-Cedam), pp. 75-115

BISI, Silvia (2005): "Il corpo come password: alcune considerazioni in tema di sistemi di autenticazione biometrica", *Cyberspazio e diritto*, 6 (4), pp. 3-35

BLAIOTTA, Rocco (2010): *Causalità giuridica* (Torino, Giappichelli)

BONETTI, Michele (2003): *Riservatezza e processo penale* (Milano, Giuffrè)

CAPRIOLI, Francesco (2009): "Scientific evidence e logiche del probabile nel processo per il 'delitto di Cogne'", *Cassazione penale*, 5, pp. 1867 e ss.

CAPRIOLI, Francesco (2008): "La scienza 'cattiva maestra': le insidie della prova scientifica nel processo penale", *Cassazione penale*, 9, p. 3523.

CECCHI, Marco (2017): "L'autonoma valutazione del giudice' quale baluardo contro l'ap-piattimento sulla prova scientifica", *Diritto Penale e Processo*, 7, pp. 915-924

CESARI, Claudia (1999): *L'irripetibilità sopravvenuta degli atti di indagine* (Milano, Giuffrè)

CORDERO, Franco, (2012): *Procedura penale* (Milano, Giuffrè)

⁶⁹ Cfr. art. 9 del Regolamento (UE) n. 2016/679.

⁷⁰ RODOTÀ (2006), pp. 3-24.

- CUOMO, Luigi (2014): “Profili giuridici del trattamento biometrico dei dati”, *Rivista Italiana di Medicina Legale e del Diritto in campo sanitario*, 1, p. 43
- DANIELE, Marcello (2011): “La prova digitale nel processo penale”, in *Rivista di diritto processuale*, pp. 297 ss.
- DOMINIONI, Oreste (2015): “L’esperienza italiana di impiego della prova scientifica nel processo penale”, *Diritto Penale e Processo*, 5, p. 601
- DOMINIONI, Oreste (2005): *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione* (Milano, Giuffrè)
- FANUELE, Chiara (2009): *Dati genetici e procedimento penale* (Padova, Cedam)
- FELICIONI, Paola (2016): Il regolamento di attuazione della banca dati nazionale del DNA: scienza e diritto si incontrano, *Diritto penale e processo*, 6, pp. 724 - 742
- FELICIONI, Paola (2009): “L’Italia aderisce al Trattato di Prum: disciplinata l’acquisizione e l’utilizzazione probatoria dei profili genetici”, *Diritto penale e processo*, 2 (2), pp. 6-24
- FELICIONI, Paola (2007): *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico* (Milano, Ipsoa)
- FERRUA, Paolo (2008): “Metodo scientifico e processo penale”, *Diritto penale e processo*, 6, pp. 12-19
- FORTE, Luca (2018): “Il ruolo della perizia nel processo penale tra neutralità della prova e prova decisiva: una difficile collocazione”, *Giurisprudenza Italiana*, 10, p. 2267
- GALGANI, Benedetta (2003): “Un test di elevata scientificità e un inedito banco di prova per la ‘civiltà’ del processo” in CHIAVARIO, Mario (eds.) *Nuove tecnologie e processo penale* (Torino, Giappicchelli), pp. 40-50
- GIUNTA, Fausto (2014): *Questioni scientifiche e prova scientifica tra categorie sostanziali e regole di giudizio*, (Pisa, Edizioni ETS)
- GRAHAM, Michael (2000): “The Expert Witness Predicament: Determing ‘Reliable’ Under the Gatekeeping Test of Daubert, Kuhmo, and Proposed Amended Rule 702 of Federal Rules of Evidence”, *University of Miami Law Review*, 317, pp. 322 e ss.
- GRAHAM Michael (1992): *Federal Rules of Evidence. A Nutshell* (St. Paul Minn., Thomson West)
- GRIMALDI Mirko, D’APOLITO Sonia, FIVELA GILI Barbara, SIGONA Francesco (2014): “Illusione e scienza nella fonetica forense: una sintesi”, *Mondo Digitale*, 13 (53), pp. 1-9
- ICHINO, Giovanna (1992): “Gli atti irripetibili e la loro utilizzazione dibattimentale”, in UBERTIS, Giulio (eds.): *La conoscenza del fatto nel processo penale* (Milano, Giuffrè), pp. 110 e ss.
- IOVANE, Gerardo (2008): *Metodi matematici e tecnologie informatiche per l’analisi delle immagini in biometria e sicurezza* (Roma, Aracne)
- KAUFMAN, Robert (2001): “The expert witness. Neither Frye nor Daubert solved the problem: what can be done?”, *Science & Justice*, 41, 1, pp. 7-20
- KOSTORIS, Roberto E. (2006): “Prelievi biologici coattivi” in KOSTORIS Roberto E. e ORLANDI Renato (eds.): *Contrasto al terrorismo interno e internazionale* (Torino, Giappicchelli), pp. 329 e ss.
- LA REGINA, Katia (2018): “Riconoscimento della voce – brevi note sul riconoscimento della voce nel processo penale”, *Giurisprudenza Italiana*, 1, 212
- LORUSSO, Sergio (2008): “La prova scientifica” in GAITO, Alfredo (eds.): *La prova penale*, (Milano, Utet), pp. 295 e ss.

MASERA, Luca (2007): “Il giudice penale di fronte a questioni tecnicamente complesse: spunti di riflessione sul principio dello iudex peritus peritorum - Il commento”, *Il Corriere del Merito*, 3 (3), pp. 351-355

MASTRANGELO, Nicolina (2017): “Profiling del DNA: una rivoluzione chiamata PCR e STRs”, *Criminalistica*, (<http://crimint.it/profiling-del-dna-una-rivoluzione-chiamata-pcr-e-strs/>)

MASTRONARDI, Giuseppe (2014): “Identificazione personale mediante il confronto di volti”, *Mondo Digitale*, pp. 1-12

MOSCARINI, Paolo (2016): “Lo statuto della ‘prova scientifica’ nel processo penale”, *Diritto Penale e Processo*, 6, pp. 649 e ss.

PREITE, Gianpasquale (2016): *Politica e biometria. Nuove prospettive filosofiche delle scienze sociali* (Trento, Tangran edizioni scientifiche)

PREITE, Gianpasquale (2007): *Il riconoscimento biometrico. Sicurezza versus Privacy* (Trento, Ed. UNI Service)

PULITANÒ, Domenico (2006): “Il diritto penale fra vincoli di realtà e sapere scientifico”, in *Rivista italiana di diritto processuale penale*, 49 (3), pp. 795-825

QUATTROCOLO, Serena (2019): “Equità del processo penale e automated evidence alla luce della convenzione europea dei diritti dell'uomo”, *Rivista Italo-Spagnola di Diritto Processuale*, 1, pp. 1-17

RENZETTI, Silvia (2015): “La prova scientifica nel processo penale: problemi e prospettive”, *Rivista di Diritto Processuale*, 2, pp. 399 e ss.

RICCI Cristoforo e RICCI Pietrantonio (2018): “Le biobanche di ricerca: questioni e disciplina”, *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)*, 1, p. 93

RICCI, Ugo (2001): *Dna e crimine: dalla traccia biologica all'identificazione genetica* (Roma, Laurus Robuffo)

RIVELLO, Pierpaolo (2016): “Alcune osservazioni in ordine alla banca dati nazionale del DNA”, *Diritto penale e processo*, 11, pp. 1521-1531

RODOTÀ, Stefano (2006): “Trasformazioni del corpo”, *Politica del diritto*, 1, pp. 3-24

SECKINER Dilan, MALLETT Xanthé, MAYNARD Philip, MEUWLY Didier, ROUX Claude (2019): “Forensic gait analysis – Morphometric assessment from surveillance footage”, *Forensic Science International*, 296, pp. 57-66

SELLAROLI, Valentina (2006): “Analisi del Dna e processo: in quale senso è una novità?” in CHIAVARIO, Mario (eds.): *Nuove tecnologie e processo penale* (Torino, Giappicheli), pp. 70 e ss.

TARUFFO, Michele (2005): “La prova scientifica nel processo civile”, *Rivista trimestrale di diritto processuale civile*, 4, p. 1079

TERRACIANO, Ugo (2014): *La metodologia dell'investigazione* (Milano, Franco Angeli)

TISTARELLI Massimo e CHAMPOD Christophe (2017): *Handbook of Biometrics for Forensic Science* (Cham, Springer)

TONINI, Paolo (2015): “Nullum iudicium sine scientia. Cadono vecchi idoli nel caso Meredith Kercher”, *Diritto Penale e Processo*, 11, pp. 1410 e ss.

TONINI, Paolo (2011): “Dalla perizia ‘prova neutra’ al contraddittorio sulla scienza”, *Diritto Penale e Processo*, 3, p. 361

TONINI, Paolo (2010a): “La Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza”, *Diritto penale e processo*, 11, pp. 1341 e ss.

TONINI, Paolo (2010b): *Manuale di procedura penale* (Milano, Giuffrè)

UBERTIS, Giulio (2016): “Prova scientifica e giustizia penale”, *Rivista italiana di diritto processuale penale*, pp. 1198 ss.

VALLI, Roberto (2013): *Le indagini scientifiche nel procedimento penale* (Milano, Giuffrè)

VANACORE, Giorgio (2015): “Sapere scientifico e processo giudiziario”, *Danno e Responsabilità*, 6, pp. 645 e ss.

WAYMAN James, JAIN Anil, MAIO Dario (2005): *Biometric Systems. Technology, Design and Performance Evaluation* (New York, Springer)

WILKINS, Jonathan (2019): “Can biometrics secure manufacturing?”, *Biometric Technology Today*, 1, pp. 9-11

YORUK Erdem, KOKUKOGLU Ender, SANKUR Bulent (2006): “Shape-Based Hand Recognition”, *IEEE Transaction on Image Processing*, 15 (7), pp. 1083-1815



Diritto Penale Contemporaneo

R I V I S T A T R I M E S T R A L E

REVISTA TRIMESTRAL DE DERECHO PENAL
A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

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