unimc
UNIVERSITÀ DI MACERATA
l'umanesimo che innova

Collana del Dipartimento di Giurisprudenza
dell'Università degli Studi di Macerata

New technologies between security and the protection of fundamental rights: a zero–sum game?

a cura di
SVEVA DEL GATTO

Editoriale Scientifica

Collana del Dipartimento
di Giurisprudenza dell'Università
degli Studi di Macerata

NEW TECHNOLOGIES BETWEEN SECURITY AND THE PROTECTION OF FUNDAMENTAL RIGHTS: A ZERO–SUM GAME?

a cura di

Sveva Del Gatto

EDITORIALE SCIENTIFICA

Volume stampato con il contributo del Dipartimento di Giurisprudenza e della Scuola di specializzazione per le professioni legali delle Università degli studi di Macerata e Camerino.

Via San Biagio dei Librai, 39 - 80138 Napoli
www.editorialescientifica.com info@editorialescientifica.com

ISBN 979-12-235-0558-8

Indice

NEW TECHNOLOGIES BETWEEN SECURITY AND THE PROTECTION OF FUNDAMENTAL RIGHTS: A ZERO–SUM GAME?

On 8, 9 and 10 July 2024, the tenth annual conference of ICON•S – The International Society of Public Law – was held at IE University in Madrid on the theme "*The Future of Public Law: Resilience, Sustainability, and Artificial Intelligence*".

The conference was an opportunity to encourage reflection and discussion on the various transformations that are taking place as a result of the great social challenges of our time: the search for sustainability, the AI revolution and, more generally, the need for resilience in an exponentially changing context. Faced with numerous transitions, sometimes in conflict with each other, scholars from around the world met to discuss the problems posed by such changes and the ability of national constitutions, state and supranational structures, and current regulatory regimes to anticipate, mitigate, and adapt to unexpected crises and challenges. In this context, the annual ICON'S Conference in Madrid was a fruitful opportunity to take stock of the role that public law, in its various branches, can (and must) still play in responding to the new challenges posed by the changes mentioned above.

As part of this Conference, the panel discussion entitled "*New technologies between security and the protection of fundamental rights: a zero–sum game?*", organised by Sveva Del Gatto and Fulvio Costantino with the participation of scholars from various disciplines, not only legal ones, focused in particular on the transformation, or rather, the revolution generated by the advent of artificial intelligence in the field of public security and the many ethical, legal and social issues that arise from it.

Global threats such as international terrorism and transnational organised crime, and new hybrid threats generated by the spread of digitalisation, are making security issues increasingly urgent and crucial, and are creating new challenges for scholars and regulators. The development of new technologies can certainly be a fundamental aid

in ensuring security and public order, but their use is not without risks and dysfunctions. The use of artificial intelligence for reasons of national and citizen security (which are not always effective) risks subjecting individuals to permanent and increasingly intense surveillance, which often involves violations of privacy, restrictions on civil rights and fundamental freedoms, and even authoritarian abuses, as in the case of Chinese social scoring.

From a cost–benefit perspective, the relationship between privacy and security is usually framed as a trade–off. However, the compromise–based approach is far from incontrovertible. It presents privacy and security as abstract categories, rather than as established social practices that emerge from the interaction between people and their social and institutional context and ends up simplifying the debate on the balance between privacy and security in an unacceptable way, reducing it to a zero–sum game. On the contrary, the protection of the right to privacy and other fundamental rights and freedoms, even in the use and development of new technologies and artificial intelligence software, is the only way to achieve the "civilised" use of such tools, as the European Data Protection Supervisor has long pointed out.

During the panel discussion, the presentations (focusing on facial recognition, social scoring, public security in smart cities and cybersecurity) sought to shed light on these issues, favouring a multidisciplinary approach that involved scholars of administrative law and criminal procedural law, engineers and data scientists.

The technocratic and authoritarian implications of emerging security policies based on new technologies, as well as the risks of functional drift, chilling effects, data commercialisation and social discrimination, were the subject of various reports.

These reports, enriched and reworked, are now contained in this volume.

The first chapter, written by Paolo Sernani and others, entitled "*Artificial Intelligence for Surveillance Applications: a Technical Perspective*", offers a technical overview of data–driven artificial intelligence applications in modern video surveillance, focusing on two crucial areas: multi–pose facial recognition and automatic detection of violence. In particular, the study evaluates the effectiveness of convolutional neural networks (specifically: VGG16, ResNet50, SENet) in identifying individuals from video surveillance footage using datasets

that simulate mug shots with variable poses, demonstrating that the inclusion of non–standard perspectives significantly improves performance. For violence detection, MobileNetV2–based architectures integrated with recurrent layers (Bi–LSTM and ConvLSTM) are introduced, optimised for use on portable and embedded devices without compromising accuracy. Experimental results on dedicated datasets confirm the practical feasibility of these approaches in public safety contexts. The chapter also addresses emerging threats related to generative artificial intelligence, such as deepfakes and facial morphing, emphasising the need for robust countermeasures and ethical safeguards to ensure the reliability and legal admissibility of AI–based surveillance systems.

The second chapter, "*Facial Recognition Technologies, Public Safety Needs, and Administrative Safeguards. A Complex Balance*" by Sveva Del Gatto, continues the reflection begun by Paolo Sernani on facial recognition but focuses, this time from a legal point of view, on issues relevant to administrative law. The contribution analyses some cases of the use of facial recognition by public administrations, both in Italy and in other jurisdictions, which have been the subject of interventions by the courts and privacy regulators.

Starting from these cases, the chapter attempts to outline, not without a critical eye, an adequate framework of principles – from legality to proportionality to transparency – that can restore balance to the relationship between public administrations and citizens when administrative power makes use of new technological tools that are as invasive and problematic as facial recognition.

Facial recognition is also addressed, this time from a criminal procedural perspective, in the third and fourth chapters written by Stefano Billi and Gaetano Galluccio Mezio, respectively.

Stefano Billi's chapter, "Riconoscimento facciale e diritti fondamentali: considerazioni di diritto processuale penale per il decimo convegno annuale "Icon'S" conference', carefully examines the impact of facial recognition systems in criminal proceedings. After a brief overview of facial recognition technologies (from traditional face detection to automated facial recognition systems, or "AFRS"), the contribution briefly describes the operating principles based on biometric templates and similarity scores, as well as the use of deep learning algorithms for identification, taking into consideration the two operating scenarios of the SARI system (enterprise and real–time)

developed to operate within the Italian legal system. Highlighting the potential benefits and risks to fundamental freedoms associated with the use of facial recognition systems, the article emphasises the critical issues of a national framework that is still incomplete, in the absence of specific rules on the processing of facial biometric data in criminal proceedings, also in light of the European Artificial Intelligence Act and given the urgent need to balance technological innovation with constitutional guarantees for the protection of individuals.

Gaetano Galluccio Mezio's contribution, "*Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*", continues on these themes, further exploring the prospects for the use of modern facial recognition technologies in criminal proceedings, with reference to both the investigative and evidentiary spheres.

The examination focuses on the legal framework of these tools, their scientific validity and epistemological suitability, as well as their debated compatibility with fundamental rights, in light of domestic regulations, relevant case law precedents and European regulations that have recently come into force.

The analysis carried out identifies significant objections regarding the legitimacy of the use of such technologies *de iure condito* but, at the same time, points to the need for a complete and thorough rethinking of the matter *de iure condendo*. From this latter perspective, the author proposes, as a guideline for future regulatory intervention aimed at achieving a fair balance between the interest in ascertaining the facts and that in respecting the fundamental principles of criminal proceedings, the possibility of regulating their use during preliminary investigations, while at the same time prohibiting their admission as evidence during the trial phase.

The problem of public safety and new technologies in relation to the protection of fundamental rights is then addressed with reference to the controversial and problematic issue of the use of social credit scoring in Fulvio Costantino's contribution entitled "*Sicurezza sociale e discriminazione sociale*". In the context of social credit scoring, public authorities can assess the social reliability of citizens by assigning them a score based on their personality traits, social behaviour and network of relationships. These mechanisms are intended as incentive systems for the adoption of virtuous behaviour, capable of bringing human behaviour towards statistical normality. However, as the au-

thor points out, these tools are, unknowingly, part of a general plan to control citizens, with an impact on personality development and the risk of limiting freedom and excluding eccentricity. The problem also arises in cases of voluntary consent, which is why it is important to reflect on the validity requirements of the consent given and the effectiveness of this guarantee for the individual and their rights.

Last but not least, given the extreme topicality of the subject, in the chapter on "*Cybersecurity Perspectives in Italy. Protecting the National Economy through New Technologies*", Patrizio Rubechini explores the prospects for cybersecurity in Italy, highlighting the importance of protecting the national economy from cyber threats. The current cybersecurity context in the country is analysed, with a focus on the challenges and opportunities for improving the resilience of critical infrastructure. The evolution of cybersecurity regulations and policies is then discussed, as well as the role of government institutions and private companies in protecting sensitive data. The text also emphasises the importance of collaboration between the public and private sectors to address emerging threats and promote a culture of cybersecurity. Finally, several recommendations are presented to strengthen national security and ensure the operational continuity of economic activities.

Sveva Del Gatto

LE NUOVE TECNOLOGIE TRA SICUREZZA E TUTELA DEI DIRITTI FONDAMENTALI: UN GIOCO A SOMMA ZERO?

L'8, il 9 e il 10 luglio 2024 si è tenuta a Madrid presso l'IE University la decima Conferenza annuale di ICON•S – *The International Society of Public Law* – sul tema "*The Future of Public Law: Resilience, Sustainability, and Artificial Intelligence*"**.**

Il convegno è stata una occasione per favorire la riflessione e il confronto sulle diverse trasformazioni che si stanno attraversando a seguito delle grandi sfide sociali del nostro tempo: la ricerca della sostenibilità, la rivoluzione dell'IA e, più in generale, la necessità di resilienza in un contesto in esponenziale mutamento. Di fronte alle numerose transizioni, a volte, peraltro, in conflitto tra loro, studiosi da tutto il mondo si sono incontrati per discutere dei problemi che siffatti mutamenti pongono e della capacità delle Costituzioni nazionali, delle strutture statali e sovranazionali e dei regimi normativi oggi vigenti di anticipare, mitigare e di adattarsi a crisi e sfide impreviste. In questo contesto, il Convegno annuale ICON'S di Madrid è stato un momento proficuo per fare il punto sul ruolo che il diritto pubblico, nelle sue diverse diramazioni, può (e deve) ancora avere nel dare risposte alle nuove sfide che i cambiamenti sopra ricordati pongono.

Nell'ambito di questa Conferenza, il panel "*New technologies between security and the protection of fundamental rights: a zero–sum game?"* organizzato da Sveva Del Gatto e Fulvio Costantino con la partecipazione di studiosi di diverse discipline, non solo giuridiche, si è concentrato, in particolare, sulla trasformazione, o meglio, sulla rivoluzione generata dall'avvento dell'intelligenza artificiale nell'ambito della sicurezza pubblica e sulle molteplici questioni, etiche, legali e sociali che ne derivano.

Le minacce globali quali il terrorismo internazionale e la criminalità organizzata transnazionale, e le nuove minacce ibride generate proprio dalla diffusione della digitalizzazione stanno rendendo sempre più urgenti e nodali le questioni legate alla sicurezza e stanno creando nuove sfide per gli studiosi e per i regolatori. Lo sviluppo delle

nuove tecnologie può certamente essere un aiuto fondamentale per garantire la sicurezza e l'ordine pubblico, ma il loro utilizzo non è privo di rischi e disfunzioni. L'utilizzo dell'intelligenza artificiale per ragioni di sicurezza nazionale e dei cittadini rischia di sottoporre gli individui a una sorveglianza permanente e sempre più intensa, che spesso comporta violazioni della *privacy*, restrizioni dei diritti civili e delle libertà fondamentali financo a derive autoritarie come nel caso del *social scoring* cinese.

Da un punto di vista costi–benefici, il rapporto tra *privacy* e sicurezza è solitamente inquadrato come un compromesso. L'approccio basato sul compromesso, tuttavia, è tutt'altro che incontrovertibile. Esso presenta la *privacy* e la sicurezza come categorie astratte, anziché come pratiche sociali consolidate che emergono dall'interazione tra le persone e il loro contesto sociale e istituzionale, e finisce per semplificare inaccettabilmente il dibattito sul bilanciamento tra *privacy* e sicurezza finendo per ridurlo a un gioco a somma zero. Al contrario, la tutela del diritto alla *privacy* e degli altri diritti e libertà fondamentali, pur nell'utilizzo e nello sviluppo delle nuove tecnologie e dei *software* di intelligenza artificiale, è l'unico modo per giungere all'uso "civilizzato" di tali strumenti come già ricordato da tempo dal Garante europeo della protezione dei dati.

Nell'ambito del *panel,* le relazioni (incentrate sui temi riconoscimento facciale, del *social scoring*, della sicurezza pubblica nelle *smart city* e della *cybersecurity*) hanno quindi provato a far luce su questi aspetti privilegiando un approccio multidisciplinare che ha coinvolto studiosi di diritto amministrativo e di diritto processuale penale, ingegneri e *data scientist*. Le implicazioni tecnocratiche e autoritarie delle politiche di sicurezza emergenti basate sulle nuove tecnologie, ma anche i rischi di deriva funzionale, effetto congelante, commercializzazione dei dati e discriminazione sociale sono stati oggetto delle diverse relazioni.

Tali relazioni arricchite e rielaborate sono ora contenute in questo Volume.

Al suo interno, il primo capitolo scritto da Paolo Sernani e altri dal titolo *"Artificial Intelligence for Surveillance Applications: a Technical Perspective"* offre una ricognizione tecnica delle applicazioni di intelligenza artificiale *data–driven* alla videosorveglianza moderna, concentrandosi su due ambiti cruciali: il riconoscimento facciale multi–posa e il rilevamento automatico della violenza. In particolare, lo

studio valuta l'efficacia di reti neurali convoluzionali (specificatamente: VGG16, ResNet50, SENet) nell'identificare individui da filmati di videosorveglianza utilizzando dataset che simulano foto derivanti dal fotosegnalamento con pose variabili, dimostrando che l'inclusione di prospettive non standard migliora significativamente le prestazioni. Per il rilevamento della violenza, vengono introdotte architetture basate su MobileNetV2 integrate con strati ricorrenti (Bi–LSTM e ConvLSTM), ottimizzate per l'uso su dispositivi portatili ed integrati, senza compromettere l'accuratezza. I risultati sperimentali su dataset dedicati confermano la fattibilità pratica di questi approcci in contesti di pubblica sicurezza. Il capitolo affronta inoltre le minacce emergenti legate all'intelligenza artificiale generativa, come i *deepfake* e il morphing facciale, sottolineando la necessità di contromisure robuste e di garanzie etiche per assicurare l'affidabilità e l'ammissibilità legale dei sistemi di sorveglianza basati sull'IA.

Il secondo capitolo "*Facial Recognition Technologies, Public Safety Needs, and Administrative Safeguards. A complex Balance"* di Sveva Del Gatto prosegue la riflessione avviata da Paolo Sernani sul riconoscimento facciale ma si concentra, questa volta da un punto di vista giuridico, sulle questioni rilevanti per il diritto amministrativo. Il contributo analizza alcuni casi di utilizzo del riconoscimento facciale da parte delle pubbliche amministrazioni, sia in Italia, sia in altri ordinamenti, su cui si sono registrati interventi delle Corti giurisdizionali e dei Garanti per la *privacy*. Partendo da questi casi, nel capitolo si prova a delineare, non senza uno sguardo critico, un adeguato quadro di principi – dalla legalità, alla proporzionalità, alla trasparenza – che possa ricondurre a un piano di equilibrio il rapporto tra pubbliche amministrazioni e amministrati quando il potere amministrativo si avvale di nuovi strumenti tecnologici così invasivi e così problematici come il riconoscimento facciale.

Del riconoscimento facciale si occupano anche, questa volta dalla prospettiva processualpenalistica, il terzo e il quarto capitolo scritti rispettivamente da Stefano Billi e da Gaetano Galluccio Mezio.

Nel capitolo di Stefano Billi "*Riconoscimento facciale e diritti fondamentali: considerazioni di diritto processuale penale per il decimo convegno annuale "ICON*" è accuratamente esaminato l'impatto dei sistemi di riconoscimento facciale nel processo penale. Dopo una breve ricognizione delle tecnologie di *facial recognition*, (dal *face detection* tradizionale agli *automated facial recognition systems* c.d. "AFRS"), il

contributo descrive sinteticamente i principi di funzionamento basati su *template* biometrici e *similarity score*, nonché l'impiego di algoritmi di *deep learning* per l'identificazione, prendendo quindi in considerazione i due scenari operativi del sistema SARI (*enterprise* e *real–time*) sviluppato per operare nell'ordinamento italiano. Evidenziate le potenzialità nonché i rischi per le libertà fondamentali a fronte dell'impiego dei sistemi di riconoscimento facciale, l'articolo pone in rilievo le criticità di una disciplina nazionale ancora incompiuta, in assenza di norme specifiche sul trattamento dei dati biometrici facciali nel processo penale, anche alla luce dell'*Artificial Intelligence Act* europeo e stante l'urgenza di bilanciare innovazione tecnologica con le garanzie costituzionali a tutela dell'individuo.

Il contributo di Gaetano Galluccio Mezio "*Tecnologie di riconoscimento facciale: una riflessione sul loro impiego con finalità investigative e probatorie*" prosegue su questi temi approfondendo ulteriormente le prospettive di impiego delle moderne tecnologie di riconoscimento facciale nel procedimento penale, con riferimento sia all'ambito investigativo sia a quello probatorio.

La disamina si sofferma sull'inquadramento giuridico di tali strumenti, sulla loro validità scientifica e idoneità epistemologica, nonché sulla loro dibattuta compatibilità con i diritti fondamentali, alla luce della disciplina interna, dei precedenti giurisprudenziali rilevanti e delle norme europee di recente entrata in vigore.

L'approfondimento svolto conduce a individuare rilevanti obiezioni in ordine alla legittimità del ricorso a tali tecnologie *de iure condito* ma, al contempo, segnala l'esigenza di un compiuto e puntuale ripensamento della materia *de iure condendo*.

Da quest'ultima prospettiva, l'Autore propone, quale linea guida di un futuro intervento normativo, finalizzato a realizzare un equo bilanciamento tra l'interesse all'accertamento dei fatti e quello al rispetto dei principi fondamentali del processo penale, la possibilità di disciplinarne l'impiego nel corso delle indagini preliminari, vietandone contestualmente l'ammissione quale prova nella fase del giudizio.

Il problema della sicurezza pubblica e delle nuove tecnologie in relazione alla tutela dei diritti fondamentali è poi declinato con riferimento al discusso e problematico tema del ricorso a modalità di *social credit scoring* nel contributo di Fulvio Costantino dal titolo *"Sicurezza sociale e discriminazione sociale"*.

Nell'ambito del *social credit scoring* le autorità pubbliche possono

valutare l'affidabilità sociale dei cittadini attribuendo loro un punteggio, sulla base delle caratteristiche della personalità, il comportamento sociale, la rete di relazioni. Tali meccanismi si pongono come sistemi di incentivazione all'adozione di comportamenti virtuosi, in grado di far convergere i comportamenti umani verso una normalità statistica.

Questi strumenti, tuttavia, come evidenziato dall'Autore, sono, inconsapevolmente, espressione di un progetto generale di controllo dei cittadini, con un impatto sulla costruzione della personalità e il rischio di limitazioni della libertà e di forme di esclusione dell'eccentricità. Il problema, peraltro, si pone anche nei casi di adesione volontaria tale per cui è importante riflettere sui requisiti di validità del consenso prestato e sull'efficacia di tale garanzia per l'individuo e i suoi diritti.

In ultimo, non per importanza, considerata l'estrema attualità del tema, nel capitolo su "*Cybersecurity Perspectives in Italy. Protecting the National Economy through New Technologies*" Patrizio Rubechini esplora le prospettive della *cybersecurity* in Italia, evidenziando l'importanza di proteggere l'economia nazionale dalle minacce informatiche. Viene analizzato il contesto attuale della sicurezza informatica nel paese, con un focus sulle sfide e le opportunità per migliorare la resilienza delle infrastrutture critiche. Si discute, poi, dell'evoluzione delle normative e delle politiche di *cybersecurity*, nonché del ruolo delle istituzioni governative e delle aziende private nella protezione dei dati sensibili. Nel testo si sottolinea, altresì, l'importanza della collaborazione tra settore pubblico e privato per affrontare le minacce emergenti e promuovere una cultura della sicurezza informatica. Infine, vengono presentate alcune raccomandazioni per rafforzare la sicurezza nazionale e garantire la continuità operativa delle attività economiche.

Sveva Del Gatto

Paolo Sernani*, Paolo Contardo**, Aldo Franco Dragoni***

ARTIFICIAL INTELLIGENCE FOR SURVEILLANCE APPLICATIONS: A TECHNICAL PERSPECTIVE

1. *Introduction*

Since its inception, Artificial Intelligence (AI) has pursued the ambitious goal of determining whether machines can be designed with the ability to think. In this ongoing exploration, symbolic AI, often referred to as Good Old-Fashioned AI[1], seeks to represent knowledge in application domains using high-level, human-readable formalizations. This approach has been widely applied across a diverse array of fields, including personal health systems[2], police investigations[3], autonomous agents[4], and

* Department of Law, University of Macerata, Macerata, Italy

** Gabinetto Interregionale di Polizia Scientifica per le Marche e l'Abruzzo, Ancona, Italy

*** Dipartimento di Ingegneria dell'Informazione, Università Politecnica delle Marche, Ancona, Italy

[1] J. Haugeland, *Artificial intelligence: The very idea*. Boston, 1989, 1 ss.

[2] N. Falcionelli, P. Sernani, A. Brugués, D. N. Mekuria, D. Calvaresi, M. Schumacher, A. F. Dragoni, and S. Bromuri, *Indexing the event calculus: Towards practical human-readable personal health systems*, in *Artificial Intelligence in Medicine*, 96, 2019, 154-166. G. Tartarisco, G. Baldus, D. Corda, R. Raso, A. Arnao, M. Ferro, A. Gaggioli, and G. Pioggia, *Personal health system architecture for stress monitoring and support to clinical decisions*, in *Computer Communications*, 35(11), 2012, 1296-1305.

[3] A. F. Dragoni and S. Animali, *Maximal consistency, theory of evidence, and bayesian conditioning in the investigative domain*, in *Cybernetics and Systems*, 34(6-7), 2003, 419-465.

[4] A. F. Dragoni, P. Giorgini, and L. Serafini, *Mental states recognition from communication*, in *Journal of Logic and Computation*, 12(1), 2002, 119-136. P. Sernani, M. Biagiola, N. Falcionelli, D. Mekuria, S. Cremonini, and A. F. Dragoni, *Time aware task delegation in agent interactions for video-surveillance*, in *Proceedings of the 1st Internatio-*

intelligent home reasoning systems[5], among many others. In parallel, machine learning has emerged as a method to equip machines with the ability to autonomously learn from examples. In this context, deep learning has experienced remarkable growth, providing computational models composed of multiple processing layers that autonomously learn optimal data representations for tasks such as speech recognition, visual object identification, and pattern recognition[6].

As advancements in AI continue to unfold, methods rooted in symbolic AI and deep learning have gained traction among law enforcement agencies for data analysis tasks[7]. In this paper, we aim to present insights from two experiments, published in our previous work, that explore AI applications in law enforcement contexts. Specifically, we focus on:

- Face Recognition, evaluating how variations in mugshot sets, including non-traditional perspectives beyond the standard frontal and profile images, influence recognition accuracy[8].
- Violence Detection, investigating approaches to automate the detection of brief violent incidents within lengthy video footage, thereby reducing the manual effort required by law enforcement personnel[9].

Although these two domains appear distinct, their computerization relies on shared foundations in Computer Vision, a field that has undergone rapid evolution with the advent of deep learning techniques. The

nal Workshop on Real-Time compliant Multi-Agent Systems co-located with the Federated Artificial Intelligence Meeting, ser. CEUR Workshop Proceedings, 2156, 2018, 16-30.

[5] D. N. Mekuria, P. Sernani, N. Falcionelli, and A. F. Dragoni, *Smart home reasoning systems: a systematic literature review*, in *Journal of Ambient Intelligence and Humanized Computing*, 12, 2021, 4485-4502. E. Serral, P. Sernani, A. F. Dragoni, and F. Dalpiaz, *Contextual requirements prioritization and its application to smart homes*, in *Ambient Intelligence*, 2017, 94-109.

[6] Y. LeCun, Y. Bengio, and G. Hinton, *Deep learning*, in *Nature*, 521(7553), 2015, 436-444.

[7] S. Raaijmakers, *Artificial intelligence for law enforcement: Challenges and opportunities*, in *IEEE Security Privacy*, 17(5), 2019, 74-77.

[8] P. Contardo, Y. F. S. Sanchez, A. F. Dragoni, and P. Sernani, *Assessing deep neural networks in face recognition using multiple mugshot sets*, in *2024 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE)*, 2024, 137-141.

[9] P. Contardo, S. Tomassini, N. Falcionelli, A. F. Dragoni, and P. Sernani, *Combining a mobile deep neural network and a recurrent layer for violence detection in videos*, in *Proceedings of the 5th International Conference on Recent Trends and Applications in Computer Science and Information Technology, ser. CEUR Workshop Proceedings*, 3402, 2023, 35-43.

experiments discussed in this paper are grounded in our prior research, which systematically evaluated the practical implications of AI techniques for surveillance applications. By presenting these experiments here, we aim to consolidate their technical insights with the aim of illustrating their broader relevance for enhancing judicial processes and operational protocols in law enforcement.

The purpose of this paper is twofold: first, to provide a detailed technical account of the methodologies and findings from our experiments; second, to highlight the broader implications of employing such technologies in judicial contexts. This includes examining the potential legal and ethical challenges raised by their use in courts, particularly in light of the capabilities introduced by Generative AI (GenAI).

The rest of the paper is structured as follows. Section 2 highlights foundational advancements in Face Recognition and Violence Detection and their relevance to the experiments presented. Section 3 discusses the effect of multi-pose datasets on Face Recognition performance, while Section 4 evaluates deep learning methodologies for violence detection in video surveillance. Section 5 considers the emerging challenges posed by Generative AI to surveillance systems, emphasizing technical, and legal implications. Finally, Section 6 synthesizes the findings and suggests directions for future research.

2. *Evolution of Face Recognition and Violence Detection Techniques*

Deep Neural Networks (DNNS) are the core of the foundational advancements in Face Recognition and violence detection. As such, we provide here a literature review about these advancements: Subsection 2.1 addresses the evolution of methodologies and technologies in Face Recognition, highlighting their growing applicability; Subsection 2.2 focuses on state-of-the-art approaches in automated violence detection.

2.1 *Face Recognition*

Face recognition has emerged as a reliable biometric identification technology, extensively applied in various domains, including passport verification[10] and smartphone authentication[11]. Its integration into these

[10] R. V. Petrescu, *Face recognition as a biometric application*, in *Journal of Mechatronics and Robotics*, 3, 2019, 237-257.

[11] K. Patel, H. Han, and A. K. Jain, *Secure face unlock: Spoof detection on smartphones*, in *IEEE Transactions on Information Forensics and Security*, 11(10), 2016, 2268-2283.

and numerous other commercial applications has been widely documented[12]. The field has experienced remarkable progress due to advancements in Deep Neural Networks (DNNs), particularly Convolutional Neural Networks (CNNs), which have proven to be highly effective in tasks such as face identification – determining whether a face image corresponds to a specific identity within a known set – and face verification, which involves assessing whether two face images belong to the same individual[13]. The efficacy of CNNs in face recognition is well-supported by existing literature. For instance, Schroff et al.[14] introduced the FaceNet system, which employs a 22-layer CNN architecture and achieved an impressive 99.63% accuracy on the LFW dataset[15]. Similarly, Taigman et al.[16] developed the DeepFace model, which utilizes an eight-layer architecture to process 152 x 152 pixel RGB images, achieving 97.35% accuracy on the same dataset. Additionally, Sun et al.[17] presented the DeepID3 framework, which reported a 99.53% accuracy on the LFW benchmark.

These contributions highlight the substantial potential of CNN-based approaches in face recognition. Furthermore, the application of pre-trained CNN models, such as VGG16, ResNet50, and SENet, has demonstrated exceptional performance through transfer learning techniques. Parkhi et al.[18] showed that the 16-layer VGG16 model, trained on the VGGFace dataset, achieved a 98.95% accuracy on the LFW images.

[12] M. O. Oloyede, G. P. Hancke, and H. C. Myburgh, *A review on face recognition systems: recent approaches and challenges*, in *Multimedia Tools and Applications*, 79(37), 2020, 27891-27922.

[13] P.-H. Lee, G.-S. Hsu, and Y.-P. Hung, *Face verification and identification using facial trait code*, in *2009 IEEE Conference on Computer Vision and Pattern Recognition*, 2009, 1613-1620.

[14] F. Schroff, D. Kalenichenko, and J. Philbin, *Facenet: A unified embedding for face recognition and clustering*, in *2015 IEEE Conference on Computer Vision and Pattern Recognition*, 2015, 815-823.

[15] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, *Labeled faces in the wild: A database for studying face recognition in unconstrained environments*, in *University of Massachusetts, Amherst, Tech. Rep. 07-49*, 2007, 1 ss. G. B. Huang and E. Learned-Miller, *Labeled faces in the wild: Updates and new reporting procedures*, in *University of Massachusetts, Amherst, Tech. Rep. UM-CS-2014-003*, 2014, 1 ss.

[16] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, *DeepFace: Closing the gap to human-level performance in face verification*, in *2014 IEEE Conference on Computer Vision and Pattern Recognition*, 2014, 1701-1708.

[17] Y. Sun, D. Liang, X. Wang, and X. Tang, *DeepID3: Face recognition with very deep neural networks*, in *CoRR*, abs/1502.00873, 2015, 1 ss.

[18] O. M. Parkhi, A. Vedaldi, and A. Zisserman, Deep face recognition, in British Machine Vision Association, 2015, 1 ss.

Similarly, Cao et al.[19] demonstrated that ResNet50, with its 50-layer architecture and residual connections, attained a top-one identification error rate of 3.9% on the VGGFace2 dataset. Likewise, You et al.[20] reported that ResNet50, pre-trained on the CASIA-Webface dataset[21], achieved a 98.58% accuracy on the LFW benchmark.

For these reasons, in Section 3, we present the findings of our research, which involves evaluating the performance of VGG16, ResNet50, and SENet on various subsets of mugshot datasets and video surveillance footage. These experiments are designed to simulate real-world scenarios encountered by law enforcement agencies, offering insights into their practical application.

2.2 *Violence Detection*

Techniques for violence detection leveraging Deep Neural Networks, particularly Recurrent Neural Networks (e.g., LSTM, Bi-LSTM, ConvLSTM) and Convolutional Neural Networks (CNNs), have also shown significant efficacy in recent studies[22]. For instance, Sudhakaran and Lanz[23] integrated spatial features extracted by 2D CNNs from video frames with a ConvLSTM to capture temporal dynamics, achieving 94.5% accuracy on the Crowd Violence dataset[24] and 97.1% on the Hockey Fight dataset[25].

[19] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, *VGGFace2: A dataset for recognising faces across pose and age*, in *2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG2018)*, 2018, 67-74.

[20] M. You, X. Han, Y. Xu, and L. Li, *Systematic evaluation of deep face recognition methods*, in *Neurocomputing*, 388, 2020, 144-156.

[21] D. Yi, Z. Lei, S. Liao, and S. Z. Li, *Learning face representation from scratch*, in *CoRR*, abs/1411.7923, 2014, 1 ss.

[22] F. U. M. Ullah, M. S. Obaidat, A. Ullah, K. Muhammad, M. Hijji, and S. W. Baik, *A comprehensive review on vision-based violence detection in surveillance videos*, in *ACM Comput. Surv.*, 55(10), 2023, 1 ss.

[23] S. Sudhakaran and O. Lanz, *Learning to detect violent videos using convolutional long short-term memory*, in *2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, 2017, 1-6.

[24] T. Hassner, Y. Itcher, and O. Kliper-Gross, *Violent flows: Real-time detection of violent crowd behavior*, in *2012 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2012, 1-6.

[25] E. Bermejo Nievas, O. Deniz Suarez, G. Bueno García, and R. Sukthankar, *Violence detection in video using computer vision techniques*, in P. Real, D. Diaz-Pernil, H. Molina-Abril, A. Berciano, and W. Kropatsch (Eds), *Computer Analysis of Images and Patterns*, Berlin, 2011, 332-339.

Similarly, Li et al.[26] proposed a 10-layer 3D CNN with dense and transitional layers, reporting 97.2% and 98.3% accuracy on the Crowd Violence and Hockey Fight datasets, respectively. Accattoli et al.[27] and Ullah et al.[28] also utilized 3D CNNs but employed transfer learning instead of training the models from scratch. Accattoli et al. combined their CNN with an SVM, attaining 99.2% accuracy on the Hockey Fight dataset and 98.5% on the Crowd Violence dataset, while Ullah et al. added fully connected layers to construct an end-to-end model, achieving 98% and 96% accuracy on the Crowd Violence and Hockey Fight datasets, respectively. Sernani et al.[29] compared 13 different deep learning models across the Hockey Fight, Crowd Violence, and AIRTLab datasets. Their results indicated that the highest accuracy was achieved using pre-trained 3D CNNs (C3D) paired with either SVMs or fully connected layers, reaching 96.1% on the AIRTLab dataset, 97.86% on the Hockey Fight dataset, and 99.6% on the Crowd Violence dataset.

Freire-Obregón et al.[30] adopted an Inflated 3D ConvNet for spatio-temporal feature extraction based on outputs from two person trackers to enable context-free violence detection. By focusing solely on individuals in the videos and excluding background information, their approach achieved 99.45% accuracy on the Crowd Violence dataset, 99.43% on the Hockey Fight dataset, and 97.54% on the AIRTLab dataset when coupled with linear regression classifiers.

While these methodologies have proven effective across various datasets for automatic violence detection, their computational and storage requirements render them unsuitable for deployment in mobile and em-

[26] J. Li, X. Jiang, T. Sun, and K. Xu, *Efficient violence detection using 3D convolutional neural networks*, in *2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, 2019, 1-8.

[27] S. Accattoli, P. Sernani, N. Falcionelli, D. N. Mekuria, and A. F. Dragoni, *Violence detection in videos by combining 3D convolutional neural networks and support vector machines*, in *Applied Artificial Intelligence*, 34(4), 2020, 329-344.

[28] F. U. M. Ullah, A. Ullah, K. Muhammad, I. U. Haq, and S. W. Baik, *Violence detection using spatiotemporal features with 3D convolutional neural network*, in *Sensors*, 19(11), 2019, 2472 ss.

[29] P. Sernani, N. Falcionelli, S. Tomassini, P. Contardo, and A. F. Dragoni, *Deep learning for automatic violence detection: Tests on the airtlab dataset*, in *IEEE Access*, 9, 2021, 160580-160595.

[30] D. Freire-Obregón, P. Barra, M. Castrillón-Santana, and M. D. Marsico, *Inflated 3d convnet context analysis for violence detection*, in *Machine Vision and Applications*, 33, 2022, 1-13.

bedded systems, essential for edge computing. In prior work[31], we demonstrated that pre-trained 2D CNNs, distributed temporally across video frames and combined with Bi-LSTM, delivered lower accuracy compared to 3D CNNs. For example, VGG16[32] combined with Bi-LSTM achieved 94.92% accuracy on the AIRTLab dataset, 95.47% on the Hockey Fight dataset, and 97.39% on the Crowd Violence dataset. Despite their lower accuracy, such models may offer an acceptable trade-off for enabling violence detection on edge devices, preserving privacy, and avoiding the need for data transmission. Motivated by this trade-off, we propose leveraging MobileNetV2[33], a 2D CNN specifically optimized for mobile applications. By time-distributing this architecture across video frames and integrating it with recurrent and fully connected layers, we aim to classify violence effectively. We evaluate two variants of this model: one using Bi-LSTM and the other employing ConvLSTM.

For the aforementioned reasons, in Section 4 we present the results of our experiments on the AIRTLab dataset for violence detection combining a 2D CNN and recurrent networks.

3. *The Effect of Mugshots from Multiple Perspectives in the Performance of Face Recognition*

To examine whether convolutional neural networks (CNNs) exhibit superior performance in face recognition when provided with a diverse set of images – beyond the standard frontal and profile views typically employed in police photo-signaling procedures – and to evaluate their efficacy in scenarios involving manually selected frames from surveillance videos, as commonly encountered in real-world applications, we utilized three architectures: VGG16 (as described in Parkhi et al.[34]), ResNet50, and SENet (both following the design presented in Cao et al.[35]). These architectures generate face embeddings, which are feature vectors encap-

[31] P. Sernani, N. Falcionelli, S. Tomassini, P. Contardo, and A. F. Dragoni, *op. cit.*, 160580-160595.

[32] K. Simonyan and A. Zisserman, *Very deep convolutional networks 17 for large-scale image recognition*, in *CoRR*, abs/1409.1556, 2015, 1 ss.

[33] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, and L.-C. Chen, *Mobilenetv2: Inverted residuals and linear bottlenecks*, in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2018, 4510-4520.

[34] O. M. Parkhi, A. Vedaldi, and A. Zisserman, *op. cit.*, 1 ss.

[35] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, *op. cit.*, 67-74.

sulating the unique characteristics of facial images. For implementation, we leveraged publicly available models from the Keras framework[36]. The pre-trained weights for VGG16 were obtained from the network described in Parkhi et al.[37], while those for ResNet50 and SENet were sourced from Cao et al.[38], utilizing the VGGFace and VGGFace2 datasets.

We conducted our experiments using the FRMDB dataset[39], which comprises 67 individuals, each represented by 28 systematically captured mugshots taken from different angles, as illustrated in Figure 1. Specific subsets of these images served as reference data for recognizing individuals in manually selected frames from surveillance videos featuring the same subjects.

For selecting facial images in our evaluation, we adhered to the European Network of Forensic Science Institutes (ENFSI) guidelines outlined in their best practices manual[40] for facial image comparison. To align our methodology with procedures employed by law enforcement, we manually selected a representative frame from each video and cropped the corresponding face. Consequently, we selected three facial images for recognition from 28 subjects (each associated with three surveillance videos) and five facial images for recognition from the remaining 39 subjects (each with five surveillance videos).

As described in our previous work[41], the performance of VGG16, ResNet50, and SENet was evaluated in terms of their ability to identify individuals in surveillance footage using subsets of mugshots as reference images. We calculated the recognition accuracy by measuring whether

[36] Available at https://github.com/rcmalli/keras-vggface

[37] O. M. Parkhi, A. Vedaldi, and A. Zisserman, *op. cit.*, 1 ss. The weights of the network are downloadable from https://www.robots.ox.ac.uk/~vgg/software/vgg_face/.

[38] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, *op. cit.*, 67-74. The weights of the network are downloadable from https://github.com/ox-vgg/vgg_face2

[39] P. Contardo, P. Sernani, S. Tomassini, N. Falcionelli, M. Martarelli, P. Castellini, and A. F. Dragoni, *FRMDB: Face recognition using multiple points of view*, in *Sensors*, 23(4), 2023, 1 ss. P. Contardo, N. Rossini, S. Tomassini, N. Falcionelli, A. F. Dragoni, and P. Sernani, *Evaluating deep neural networks for face recognition with different subsets of mugshots from the photo-signaling procedure*, in *2023 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE)*, 2023, 543-548.

[40] *Best Practice Manual for Facial Image Comparison Version 01, European Network of Forensic Science Institutes (ENFSI)*, 2018, Available: https://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf.

[41] P. Contardo, P. Sernani, S. Tomassini, N. Falcionelli, M. Martarelli, P. Castellini, and A. F. Dragoni, *op. cit.*, 1 ss.

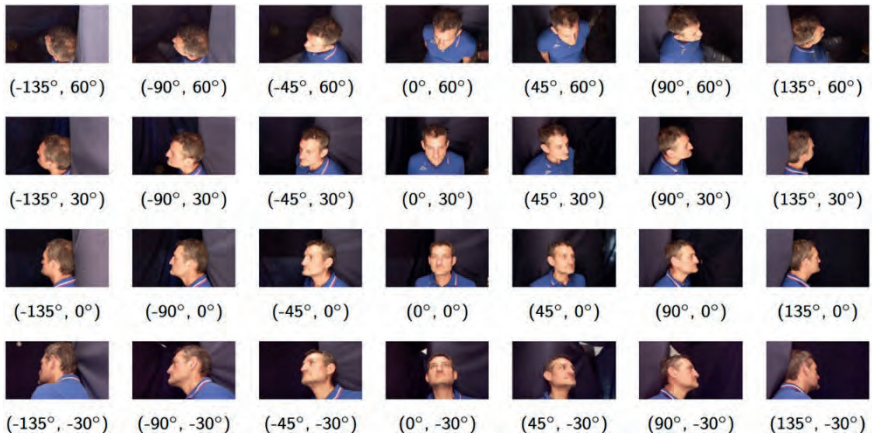

Figure 1. The 28 mugshots available for a subject in the FRMDB. For each mugshot, the angles from which the picture was taken are reported as a couple (h, v): h is the angle on the horizontal plane from -135° to +135°, with an increment of 45° between an angle and its adjacent (from left to right); v is the angle on the vertical plane from 60° to -30°, with a step of -30° between an angle and its adjacent (from top to bottom).

the correct subject appeared among the top-1, top-3, top-5, or top-10 most similar mugshots (or identities) identified by the CNNs. These networks encode facial images into embeddings, and we measured the similarity between embeddings using the Euclidean distance. Our metrics assessed the proportion of surveillance video frames in which the correct subject appeared within the ranked top-1, top-3, top-5, or top-10 identities, relative to the total number of such frames.

Regarding the reference mugshots used for recognition, Table 1 outlines the subsets of images employed to compare the performance of VGG16, ResNet50, and SENet in identifying individuals depicted in surveillance videos.

Table 1. The image subsets for each individual in the FRMDB serve as reference points for facial recognition within security footage. Each subset is named and detailed by the angles at which the photos were captured. Specifically, the angles in the mugshots are denoted as a pair *(h, v)*, where *h* represents the horizontal plane angle, and *v* denotes the vertical plane angle.

Subset	**Included mugshots (horizontal plan, vertical plane)**
"Test F"	(0°, 0°)
"Test F-L1-R1"	(0°, 0°), (–45°, 0°), (45°, 0°)

"Test 1"	(0°, 0°), (90°, 0°)
"Test 2"	(0°, 0°), (90°, 0°), (–90°, 0°)
"Test 3"	(0°, 0°), (90°, 0°), (–90°, 0°), (45°, 0°), (45°, 0°)
"Test 4"	(0°, 0°), (135°, 0°), (–135°, 0°), (90°, 0°), (–90°, 0°), (45°, 0°), (45°, 0°)
"Test 5"	(0°, 0°), (135°, 0°), (–135°, 0°), (90°, 0°), (–90°, 0°), (45°, 0°), (45°, 0°), (0°, 30°), (135°, 30°), (–135°, 30°), (90°, 30°), (–90°, 30°), (45°, 30°), (45°, 30°)
"Test 6"	(0°, 0°), (135°, 0°), (–135°, 0°), (90°, 0°), (–90°, 0°), (45°, 0°), (45°, 0°), (0°, 30°), (135°, 30°), (–135°, 30°), (90°, 30°), (–90°, 30°), (45°, 30°), (45°, 30°), (0°, 60°), (135°, 60°), (–135°, 60°), (90°, 60°), (–90°, 60°), (45°, 60°), (45°, 60°), (0°, –30°), (135°, –30°), (–135°, –30°), (90°, –30°), (–90°, –30°), (45°, –30°), (45°, –30°)

In our study, we employed the VGG16, ResNet50, and SENet convolutional neural networks to evaluate the effectiveness of face recognition across various data subsets within the FRMDB dataset. This process involved generating facial embeddings for a total of 1896 mugshots. Additionally, we extracted frames for testing from high- and low-resolution security videos. Specifically, for 28 subjects, one frame from each of three high-resolution videos was used, and for 39 subjects, one frame from each of five low-resolution videos was processed. This resulted in a total of 279 video frames being utilized for face recognition. The embeddings derived from these frames were then compared with those generated from the corresponding mugshot subsets to assess recognition accuracy.

Figure 2 illustrates the accuracy metrics achieved by the three neural networks – VGG16, ResNet50, and SENet – on the FRMDB dataset under various ranking scenarios, with frames selected from video surveillance footage. Several notable observations emerged from our analysis. ResNet50 consistently outperformed the other networks in accuracy across all tests and rankings. VGG16, on the other hand, exhibited the lowest accuracy in every scenario. ResNet50 and SENet demonstrated generally comparable performance, with only minor variations. Tests labeled F-L1-R1, 3, 4, 5, and 6 achieved the highest accuracy values across all networks and rankings, while Test 1 recorded the lowest accuracy values. Importantly, from Test 3 onward, increasing the number of mugshots in the dataset yielded negligible improvements in accuracy.

Compared to our previous work, these experiments underscore a notable enhancement in face recognition accuracy when frames from video surveillance are selected to include profiles similar to those in the mug-

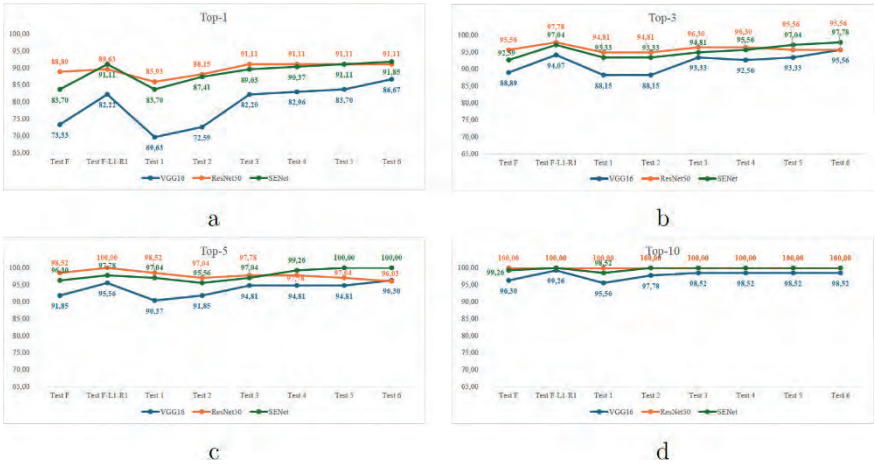

Figure 2. The accuracy measures for VGG16, ResNet50 and SENet models on the FRMDB: the top-1 identities (a), top-3 (b), top-5 (c), and top-10 (d).

shots. As shown in Figure 2, accuracy values for all networks and rankings are higher when these pose-matched profiles are included. Notably, starting from Test 3 – which incorporates the standard mugshot alongside +45° and -45° rotated profiles and a left-side profile at 90° – we observed a significant accuracy increase compared to Test 1. Adding more profiles beyond this configuration yielded limited additional improvements, indicating diminishing returns.

Our research seeks to propose a refined operational protocol for law enforcement agencies to enhance their photo-signaling procedures. This involves assessing the trade-off between the benefits of incorporating additional mugshot profiles and the associated costs of increased storage and equipment requirements. Tests such as F, which include only the frontal view, and F-L1-R1, while achieving relatively high accuracy, lack the right-side profile at 90°, which is integral to current police photo-signaling standards. Based on our findings, Test 3 emerges as the optimal configuration, as adding more profiles beyond this setup does not substantially enhance performance.

4. *Violence Detection with Deep Neural Networks*

As outlined in our previous research[42], we designed two Deep Lear-

[42] P. Contardo, S. Tomassini, N. Falcionelli, A. F. Dragoni, and P. Sernani, *op. cit.*, 35-43.

ning-based classifiers to differentiate videos as violent or non-violent. These classifiers employ MobileNetV2, pre-trained on the ImageNet dataset[43], as a feature extractor, followed by either a Bi-LSTM or a ConvLSTM layer, and fully connected layers for classification (Figure 3). The MobileNetV2 weights were frozen during training to retain the knowledge acquired from ImageNet, while the Bi-LSTM or ConvLSTM layers and the fully connected layers were trained from scratch using the AIRT-Lab dataset[44]. To ensure consistency with prior studies[45], we processed the videos in 16-frame chunks, facilitating a fair comparison among classifiers by maintaining uniformity in experimental conditions.

The Bi-LSTM-based classifier comprises 66,648,385 parameters in total, with 64,390,401 trainable parameters. These trainable parameters include the 128 hidden units of the Bi-LSTM, the 128 ReLU neurons in the first fully connected layer, and the sigmoid neuron in the final layer. By contrast, the ConvLSTM-based model contains 5,764,929 parameters, of which 3,506,945 are trainable. These correspond to the 64 filters of the ConvLSTM layer, the 256 ReLU neurons in the first fully connected layer, and the sigmoid neuron for the output. The reduced memory requirements of the ConvLSTM model make it better suited for deployment on mobile and embedded devices compared to the Bi-LSTM model.

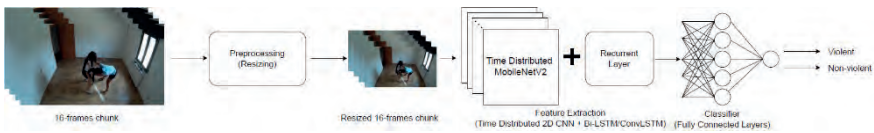

Figure 3. Schematic of the proposed models, which process 16-frame sequences resized to 224 × 224 pixels. MobileNetV2, applied as a time-distributed 2D CNN, extracts spatial features, followed by a recurrent layer (Bi-LSTM or ConvLSTM) to capture temporal features. Fully connected layers classify the videos as violent or non-violent.

[43] O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. Bernstein, A. C. Berg, and L. Fei-Fei, *ImageNet Large Scale Visual Recognition Challenge*, in *International Journal of Computer Vision (IJCV)*, 115(3), 2015, 211-252.

[44] M. Bianculli, N. Falcionelli, P. Sernani, S. Tomassini, P. Contardo, M. Lombardi, and A. F. Dragoni, *A dataset for automatic violence detection in videos*, in *Data in Brief*, 33, 2020, 106587 ss.

[45] S. Accattoli, P. Sernani, N. Falcionelli, D. N. Mekuria, and A. F. Dragoni, *op. cit.*, 329-344. P. Sernani, N. Falcionelli, S. Tomassini, P. Contardo, and A. F. Dragoni, *op. cit.*, 160580-160595.

To evaluate the performance of these classifiers and compare them with our earlier work, we conducted accuracy tests on the AIRTLab dataset. This dataset consists of 350 MP4 videos encoded with H.264, each averaging 5.63 seconds in length. Videos were recorded at 30 frames per second with a resolution of 1920 × 1080 pixels. The dataset is divided into 230 violent and 120 non-violent videos. The violent category includes 115 distinct actions recorded from two separate camera angles, while the non-violent category consists of 60 distinct actions, also recorded from two angles. All recordings took place in a single room, with one camera positioned in the top left corner opposite the door and the other in the top right corner adjacent to the door.

The videos feature non-professional actors simulating various violent and non-violent actions. Each video involved two to four actors. Violent actions depicted in the dataset include scenarios common in physical altercations, such as punching, kicking, hitting with objects, slapping, firing guns, and stabbing. The non-violent category includes actions that might trigger false positives due to their resemblance to violent activities, particularly because of rapid movements. Examples of non-violent actions are exulting, hugging, gesticulating, clapping, and giving high fives.

Since MobileNetV2 was pre-trained on the ImageNet dataset and its weights were frozen during training, the Bi-LSTM and ConvLSTM layers, along with the fully connected layers, required training from scratch. To achieve this, we employed a stratified shuffle split cross-validation strategy. Specifically, we performed a randomized 80-20 split of the dataset five times, designating 80% of the data as the training set and 20% as the test set. In each split, the class distribution was preserved to ensure a balanced representation of samples. The same data splits were applied to both our proposed models and the models from our previous work, enabling a fair comparison of performance. Given that the models take sequences of 16 frames as input and the AIRTLab dataset consists of 3537 such sequences, each split included 2829 samples for training and 708 samples for testing. Furthermore, 12.5% of the training set, equivalent to 10% of the entire dataset, was used as validation data. To match the input requirements of the original MobileNetV2 implementation, all video frames from the AIRTLab dataset were resized to 224 × 224 pixels.

Both models proposed in this study utilized the Binary Cross-Entropy loss function, which was minimized using the Adam optimizer. Training was halted early if no improvement in the minimum validation loss was observed after five consecutive epochs, with the model's weights restored to those corresponding to the epoch with the best performance.

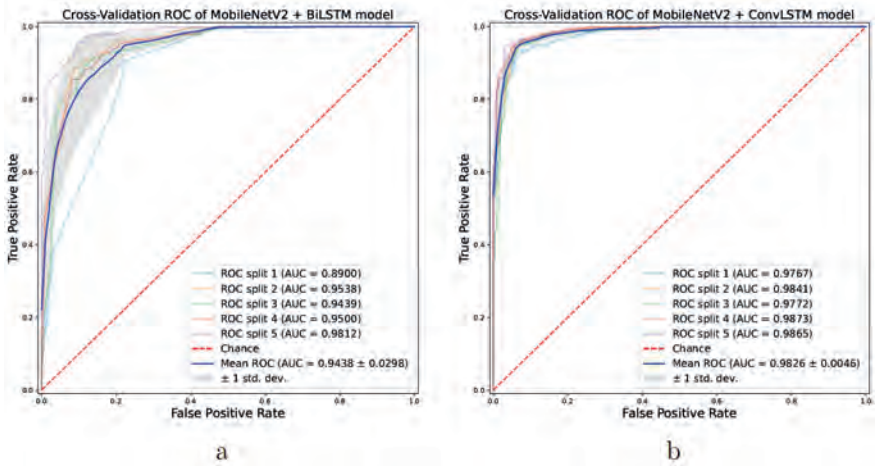

Figure 4. ROC curves and AUC values for the MobileNetV2 with Bi-LSTM (a) and MobileNetV2 with ConvLSTM (b) classifiers.

On average, the training process spanned 22.4 epochs (±5.68) for the model employing the Bi-LSTM layer and 17.8 epochs (±4.21) for the model incorporating the ConvLSTM. For both neural networks, the batch size was set at 8.

The generalization capabilities of the two models are distinctly illustrated by the ROC curves in Figure 4. The Bi-LSTM-based model achieved an average AUC of 94.38% (±2.98%), while the ConvLSTM-based model scored 98.26% (±0.46%), indicating superior accuracy in our experiments. This disparity may stem from the considerable difference in the number of trainable parameters between the two architectures. Specifically, the Bi-LSTM-based model comprises 64,390,401 trainable parameters, whereas the ConvLSTM-based model includes only 3,506,945. The larger parameter set of the Bi-LSTM model suggests potential overfitting for the violence detection task on the AIRTLab dataset, hindering its convergence to optimal classification performance. In contrast, the ConvLSTM model, being more resource-efficient, demonstrated superior classification accuracy and generalization capability.

5. *The Challenges of Generative AI*

Generative Artificial Intelligence (GenAI) has emerged as a transformative yet challenging technology in the context of video surveillance. Its

capabilities extend beyond creating realistic synthetic data to actively undermining the reliability of established AI-based recognition systems. For example, Face morphing represents a prominent threat to biometric systems. This technique involves synthesizing an image that blends the facial features of two or more individuals, often used to bypass facial recognition systems by deceiving them into recognizing multiple identities as a single individual[46]. Such attacks undermine the reliability of security frameworks that depend on facial biometrics, raising concerns about their use. Counteracting face morphing requires the development of robust detection algorithms capable of distinguishing synthetic alterations from authentic images, a task that becomes increasingly complex as generative models grow more sophisticated[47].

Deepfakes, another product of generative AI, amplify challenges in violence detection systems. Deepfakes involve synthetically altering video footage, often substituting the faces or actions of individuals within a scene[48]. These alterations pose significant hurdles for automated violence detection, as they can fabricate scenarios that lead to false positives or negatives. For instance, a benign action may be digitally modified to simulate aggression, misleading AI models into misclassifying the event. Conversely, genuine acts of violence may be obscured or replaced with non-violent imagery. Addressing these issues requires integrating forgery detection mechanisms into violence recognition pipelines, ensuring the integrity of analyzed content.

The concept of "vishing" (voice phishing) further illustrates generative AI's disruptive potential. By employing advanced voice synthesis models, malicious actors can convincingly impersonate individuals to deceive targets[49]. While predominantly a cybersecurity concern, vishing also intersects with video surveillance when audio channels are used in conjunction with visual monitoring to enhance situational awareness.

[46] M. Ferrara, A. Franco, and D. Maltoni, *Face morphing detection in the presence of printing/scanning and heterogeneous image sources*, in *IET Biometrics*, 10(3), 2021, 290-303.

[47] N. Di Domenico, G. Borghi, A. Franco, M. Ferrara, and D. Maltoni, *A framework to improve the comparability and reproducibility of morphing attack detectors*, in *2023 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE)*, 2023, 525-530.

[48] M. S. Rana, M. N. Nobi, B. Murali, and A. H. Sung, *Deepfake detection: A systematic literature review*, in *IEEE Access*, 10, 2022, 25494-25513.

[49] J. Figueiredo, A. Carvalho, D. Castro, D. Gonçalves, and N. Santos, *On the feasibility of fully AI-automated vishing attack*, in *CoRR*, abs/2409.13793, 2024, 1 ss.

The convergence of these domains necessitates multi-modal solutions capable of identifying synthesized voices alongside deepfakes in video streams.

As such, in judicial contexts, the integration of AI-based recognition techniques should face heightened scrutiny. The admissibility of evidence derived from AI systems is complicated by generative AI's ability to fabricate indistinguishable face images and videos. From a technical perspective, the main challange that evidence presented in court is authentic and free from manipulation.

Generative AI's dual-use potential exemplifies its profound implications for video surveillance. While it offers avenues for advancement in synthetic data generation and scenario simulation, its misuse undermines the reliability and trustworthiness of critical applications. Addressing these challenges necessitates a multi-disciplinary approach encompassing technical innovation, regulatory oversight, and public awareness to safeguard the integrity of AI systems in high-stakes environments.

6. *Conclusions*

In this work, we have explored the application of AI and, specifically, Deep Neural Networks to critical tasks in surveillance, focusing on multi-pose face recognition and automated violence detection. Our analysis highlights the technical efficacy of convolutional and recurrent neural networks in these domains, but the operational limitations and ethical considerations inherent in such applications should be addressed.

In particular, the capacity to generate highly realistic synthetic identities or manipulate video streams raises concerns about pervasive surveillance systems that may infringe upon individuals' privacy (on this point see, for example, Del Gatto[50]). Additionally, the potential for unauthorized synthesis or misuse of biometric data could lead to significant breaches of trust and erosion of public confidence in surveillance technologies. Such risks demand robust mechanisms for safeguarding data integrity and ensuring accountability in the deployment of AI systems.

Our experimental findings provide nuanced insights. In face recogni-

[50] S. Del Gatto, *Il riconoscimento facciale. a che punto siamo?*, in *Giornale di Diritto Amministrativo*, 5, 2022, 692-700. S. Del Gatto, *La "governance" delle nuove tecnologie tra tentativi di regolazione e istanze di "self regulation". Il caso del riconoscimento facciale*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 1, 2023, 37-64.

tion, the use of subsets from the FRMDB dataset demonstrates the potential of pre-trained CNNs like ResNet50 and SENet to achieve notable accuracy improvements with appropriately diverse image sets. However, the dataset's limited size constrains the generalizability of these results. In violence detection, the ConvLSTM-based approach proved more resource-efficient and accurate than alternatives, yet reliance on controlled datasets such as AIRTLab highlights a gap in real-world applicability.

Future research must address these limitations, including broader datasets for face recognition, mobile deployment evaluations for violence detection models, and effective aggregation strategies for long-form video analysis. Additionally, advancements in countering synthetic media threats, such as deepfakes and morphing, remain critical to preserving the reliability of AI systems in surveillance.

By addressing these challenges, AI technologies can better align with ethical standards and operational demands, ensuring they serve as reliable tools for enhancing public safety without compromising individual rights.

Acknowledgements

The presented research has been part of the Memorandum of Understanding between the Università Politecnica delle Marche, Centro "CARMELO" and the Ministero dell'Interno, Dipartimento di Pubblica Sicurezza, Direzione Centrale Anticrimine della Polizia di Stato.

Sveva Del Gatto

FACIAL RECOGNITION TECHNOLOGIES, PUBLIC SAFETY NEEDS AND ADMINISTRATIVE SAFEGUARDS. A COMPLEX BALANCE.

1. *Introduction*

The actions of public administration, including those of an authoritative nature, and the relationship between public administration and private subjects, citizens and businesses, have long been affected by profound changes. These are gradually leading to a rethinking of the traditional "authority-freedom" relationship with a view, if not to equality, certainly to a fairer balancing. On the one hand, the reforms that in recent decades have affected the Italian administrative system and the judicial review of public administration helped transform the position of the citizen with regard to the actions of public power; on the other, they contribute to reducing the deep mistrust that characterised public opinion towards public administration until the recent past.[1]

In this process of change, which is still ongoing, a central and disruptive role is destined to be played, not necessarily with always positive outcomes, by the rapid spread of new technologies and artificial intelligence also in public decision-making and in the delivery of new digital public services to citizens. Public administrations have been affected, especially in recent years, by a significant digitization process, which has

[1] F. Benvenuti, *Appunti di diritto amministrativo. Parte generale,* IV ed., Padova, 1959, pp. 183 ff. As noted by the Author: if one wished to introduce a notation of a psychological-social nature, one could say that the citizen's hostility toward the administration, the deep distrust depends precisely on the fact that just as the citizen feels, in substance, unprotected, in the same way the authority feels itself absolved of all responsibility.

been accelerated thanks to the investments included in the National Recovery and Resilience Plan (NRRP)[2]. This process, which is changing the public administration, improving its tools is bringing a gain in efficiency internal to offices and external to citizens-users. The usefulness of algorithms as a new "operational mode of management of the public interest" is appreciated, as noted by the administrative judge[3], with particular reference to all those serial or standardized procedures that the public administration is faced with and that involve the processing of large amounts of instances and the acquisition of certain and objectively verifiable data. In these cases, algorithms appear to be the tools of choice for correcting the distortions and imperfections that typically characterize cognitive processes and choices made by humans, and for speeding up and improving the activity performed. However, the use of artificial intelligence software is possible even for discretionary choices, as indicated by the Council of State itself and long admitted in doctrine[4].

Nevertheless, with regard to the relationship between public authorities and citizens, the use of algorithms is not neutral especially when it pertains to the issuance of administrative measures likely to affect the legal sphere of the recipient. Important and different, depending on the type of technology used and the activity carried out, are the problems and critical issues that must be confronted. The many benefits (especially

[2] See Component 1, Mission 1 of the National Recovery and Resilience Plan. In this direction also, Artificial Intelligence Strategic Program 2022-2024 and 2024-2026. The goal of digitizing public administration aims to improve services and performance for users and simplify relations between citizens and public administration in the belief that public administration can and should be an engine of development for the country, an ally of economic operators and not an obstacle. On these profiles see D.U. Galetta, *Transizione digitale e diritto ad una buona amministrazione: fra prospettive aperte per le Pubbliche Amministrazioni dal PNRR e problemi ancora da affrontare*, in *Federalismi.it*, 7, 2022. On the nature of the National Recovery and Resilience Plan, see M. Clarich, *Il PNRR tra diritto europeo e nazionale: un tentativo di inquadramento giuridico,* in *Corr. giur.*, 2021, pp. 1025 ff.

[3] Cons. Stato, Sec. VI, April 8, 2019, no. 2270. On the jurisprudential evolution on the subject M.C. Cavallaro, G. Smorto, *Transizione digitale della pubblica amministrazione in Italia e diritto ad una buona amministrazione: fra prospettive aperte dal PNRR e problemi tuttora da affrontare*, in *federalismi.it*, 2019, pp. 11 ff.

[4] Developments in case law, however, indicate the use of algorithms even in discretionary procedures as possible and useful. On this point the doctrine is divided. On the subject, see E. Carloni*, I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm.*, 2020, pp. 271 ff.; see also L. Torchia, *Lo Stato digitale. Un'introduzione,* Bologna, Il Mulino, 2023*, passim*.

in terms of gaining efficiency) that can be derived from the use of artificial intelligence in the exercise of public functions and services are, in fact, counterbalanced by the concrete risk of a significant infringement for the principles and guarantees towards public administrations.

This is especially true when the technology used falls within the facial recognition technologies that are receiving great interest from public administrations, especially local governments, as well as scholars.

The following paragraphs will therefore focus on facial recognition technologies, characteristics and operation. The problems that such systems pose especially when used by public administrations will be also analysed. Possible corrective measures will then be critically discussed, taking a cue from the (few) solutions developed by case law, decisions by privacy authorities and the regulation, referring not only to the Italian system but also to other systems in which the issue of the risks posed by facial recognition has been raised. Finally, some summary considerations will be made.

2. *Facial recognition systems: brief description of their operation and uses*

Facial recognition technology extracts and processes an individual's biometric data[5] creating a "biometric template". The possible uses of this

[5] The definition of biometric data provided by Article 4(1)(14) of the GDPR shows that it is: '*personal data obtained by specific technical processing relating to physical, physiological or behavioural characteristics of a natural person that enable or confirm his or her unambiguous identification, such as facial image or dactyloscopic data*'; in essence, what is relevant is the way in which the data of a person's face image is processed. Images of people's faces represent biometric data, insofar as they are capable of communicating information such as an individual's ethnic or racial origins, fall under the GDPR into the 'special categories of personal data' or sensitive data, which are accorded greater protection and additional safeguards than other personal data. In addition to the observed definition in the GDPR, biometric data are defined as '*special categories of personal data*' by Article 1(1) of the EU - Law Enforcement Directive. A special category in that from these data one has peculiar information about the individual from whom the data are extracted they reveal important aspects such as the mentioned ethnic and racial origins, membership in a religious or political group. Data capable of uniquely and unequivocally identifying an individual, such as data concerning his or her health or, again, sexual orientation, as also suggested by a reading of Art. 9 para. 1 of the GDPR. Similarly, such categories of data are also considered "special" in other jurisdictions. See for example the Australian case: here facial images and facial fingerprints are considered as sensitive information covered by additional protections under the Privacy Act 1988 because they are "biometric information used for the purpose of automated biometric identification." Biometric data have been referred to as an "umbrella concept" because, within this definition, very different types of data are

technique[6] are many[7]: from identification (or one-to-many comparison)[8] to verification (or one-to-one comparison)[9]. In addition to verification and identification, facial recognition can also be used for profiling individuals, as it allows certain characteristics such as gender, age and ethnic origin to be extracted from facial images. In this case, it is referred to as "categorization" to mean that the technology is not used to identify or match individuals, but their characteristics[10].

In recent years, facial recognition technology has spread rapidly in both the private and public sectors[11]: from object and person detection,

concentrated. J.D. Woodward, *Biometrics: A Look at Facial Recognition*, *Documented Briefing Rand Corporation*, DB-396-PSj, 293. Two main categories can be traced one referring to physiological and the other to behavioural data. Within the first classification we find devices capable of recognizing fingerprints, the geometry of our hands, and, again, smell, iris or face. The second, on the other hand, refers to the collection of information about behaviour, voice recognition, signature analysis (GDPR).

[6] Facial recognition belongs to the branch of deep learning and consists of automatic processing of digital images containing faces of individuals. In general, on facial recognition see E. Kindt, *Privacy and Data Protection Issues of Biometric Applications A comparative legal analysis* (1st edn. Springer, *Governance and Technology Series* 12, 2013); I. Iglezakis, *EU Data protection legislation and case-law with regard to biometric application*, Aristotle University of Thessaloniki, June 18, 2013.

[7] Art. 29, *Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services*, 00727/12/EN, WP 192, Brussels, March 22, 2012, 2; see also J.P. Woodward and Rand Corporation, *Facial Recognition: Defining Terms to Clarify Challenges*, November 13, 2019.

[8] Identification means that a person's facial image is compared with many other patterns stored in a database to find out whether his or her image is stored there. Facial recognition technology returns a score for each comparison and indicates the probability that two images refer to the same person. Sometimes images are matched against databases where it is known that the reference person is in the *database* (closed-set identification) and sometimes where this is not known (*open-set* identification). The latter operation would be applied when people are compared to *watchlists*.

[9] Facial recognition technology compares the two facial images, and if the probability that the two images show the same person is above a certain threshold, the identity is verified. Verification does not require biometric characteristics to be deposited in a central database. They can be stored, for example, on a card or in a person's identity/travel document. For a greater degree of detail on how this technology works, please refer to chapter 1 by Paolo Sernani in this book.

[10] If, however, the various characteristics are inferred from a face and potentially linked to other data (e.g., location data), identification of an individual could in fact be obtained as well.

[11] According to *The Global Expansion of AI Surveillance* study, edited by the *Carnegie Endowment for Institutional Peace*, 43 percent of states (precisely 64 out of a baseline sample of 176 states) used facial recognition technologies for surveillance purposes in 2019.

to access control to public and private buildings; from group demographic analysis to emotion analysis. The face can be used to unlock the *smartphone*, can be detected by CCTV cameras to enter offices or gyms, or to speed up *e-boarding* procedures at many airports. Of facial recognition there are known uses for commercial purposes, for example to record customer satisfaction levels, in the context of so-called *emotive marketing*, and also in the area of personnel where it can be used to identify, during a job interview, specific characteristics of the person for the purpose of recruitment.

Among the public administrations, facial recognition is now widely used: from schools, public housing, transportation to the public safety sector (in the species of public order, immigration and asylum).

In education, for example in Sweden and Marseille[12], facial recognition has been used to control and monitor student and visitor access and to quickly identify potential security risks. Still, the facial recognition technique is used to check attendance, assess students' attention or emotional state, and monitor examinations.

In the field of transportation, facial recognition technology is used to control access. In China, facial recognition systems are placed at bus stops and train entrances and are used to scan passengers' faces in place of physical tickets or digital ticket codes. Similar uses are being piloted in Kazakhstan.

In Russia, Face Pay is a system for accessing the Moscow subway simply by showing your face. In New York, facial recognition has been tested on bridges and tunnels to identify drivers with suspended licenses, to detect traffic violations, and to verify the driver's licenses of vehicle occupants.

Staying in the United States, facial recognition is being used in Detroit and New York City to monitor and regulate entry to public housing complexes. In Russia, Moscow's local government has announced the

East and Pacific Asia are the areas where there is-at least so far-the most widespread use of such technology (nearly 70 percent of states use it), while in the Europe and Eurasia region less than 40 percent of countries have adopted facial recognition technologies for surveillance purposes. Procuring this kind of technology and investing in its implementation are not only authoritarian systems. The interesting finding from the Report is that it is precisely liberal democracies that are the main users of facial recognition technologies, with a deployment rate of 51 percent of the total sample, compared with the lowest rate of 37 percent recorded in autocratic-type regimes. This means that one in two democratic states uses facial recognition devices for purposes-even in the broadest sense-of surveillance.

[12] See *infra* § 4.

citywide implementation of real-time facial recognition on public CCTV cameras and surveillance systems at entrances to most apartment buildings.

Facial recognition technology has been used to increase the deployment of national digital identity systems by offering help in digitizing public administration and improving the operation of digital services. For example, the State of Singapore has implemented SingPass facial recognition technology, one of the most advanced national digital identity programs in the world, which is used by residents to take advantage of numerous digital services, both private and governmental (including accessing tax returns and applying for public housing)[13].

However, the areas in which facial recognition technology appears to be most widely used are immigration and asylum and public safety. There are numerous examples in this field from different jurisdictions. In the United States, U.S. Customs and Border Protection uses facial recognition technology to screen people seeking admission to the United States. In the United Kingdom, the Home Office and the Ministry of Justice are reportedly planning to require immigrants convicted of criminal offenses to use facial recognition smartwatches[14]. The European Union uses facial recognition technology similar to the Biometric Exit Program at ports of entry to verify the identity of people applying for visas and asylum.

Facial recognition technology is used by law enforcement agencies in several countries to support investigations with the aim of making them faster and more effective, for example, in the search and capture of suspects or to find missing persons. In Italy, the S.A.R.I (automatic image recognition system) has been active since 2018. It allows the search for faces, otherwise unknown, by drawing on photos taken during mug shots (AFIS database) for comparison, automating the related search opera-

[13] The launch of the new feature, called *SingPass Face Verification*, is part of the government's US$2.4 billion (US$1.75 billion) *Smart Nation* initiative, launched in 2014, to digitize government services (from cashless payment systems to sensor-enabled street lighting). The new system was jointly developed by iProov, a UK-based biometric authentication provider and a Singapore-based digital government service platform provider. On the topic S. Del Gatto, *Riconoscimento facciale e uso dei servizi governativi. Numerosi benefici, ma quanti i rischi?,* su Osservatorio sullo Stato Digitale, IRPA, available at https://www.irpa.eu/riconoscimento-facciale-e-uso-dei-servizi-governativi-numerosi-benefici-ma-quanti-i-rischi/.

[14] The news reported by *The Guardian* newspaper can be read at https://www.theguardian.com/politics/2022/aug/05/facial-recognition-smartwatches-to-be-used-to-monitor-foreign-offenders-in-uk.

tions[15]. Facial recognition technology for law enforcement purposes is mainly used for face identification, whereby images obtained from police or private sources[16] are compared with a pre-existing database of images. Nevertheless, in some non-EU countries, facial recognition has also been used as an aid in interrogation techniques in order to understand from facial expressions whether or not the individual is telling the truth[17].

3. *The use of facial recognition technologies between guarantees of efficiency and risks of breaching fundamental rights*

The spread of facial recognition technologies brings with it many benefits as the examples just given suggest. Biometrics, in which facial recognition falls, provides higher levels of assurance that the person trying to access a service or perform a transaction is real. In addition, unlike the face, passwords, PINs and other personally identifiable information can be compromised by data breaches, allowing illegal access to accounts using traditional authentication methods. This is an undoubted advantage when we think about the digitization of services offered by public administrations.

States that take advantage of emerging technologies can provide more efficient services, reducing costs and freeing up resources to invest precisely in new digital infrastructure. This is coupled with the significant

[15] SARI is able, from a photographic image (taken from cameras on the street and videos made by officers) of an "unknown subject", to perform a computerized search both in the A.F.I.S. database (the law enforcement identification system) and on social media (where some of the boys in the pack posted comments the day after the attacks in the square in Milan). And thanks to two facial recognition algorithms, it is able to provide a list of images according to a degree of similarity. On the SARI system see V. Bontempi, *Un'interrogazione parlamentare sull'uso del riconoscimento facciale in Italia: il caso S.A.R.I.,* su Osservatorio sullo Stato Digitale, IRPA, available at https://www.irpa.eu/uninterrogazione-parlamentare-sulluso-del-riconoscimento-facciale-in-italia-il-caso-s-a-r-i/.

[16] Consider the well-known *Clearview* case on whose multiple events we refer to C. Ramotti, *Clearview A.I. approda in Italia?*; Ead., *Il caso Clearview e il Primo Emendamento alla Costituzione americana;* Ead., *Clearview A.I. cita in giudizio i dissidenti,* all of which can be consulted *online* on the Digital State Observatory, IRPA.

[17] As reported by A. M. Ousmane, T. Djara, W. Zoumarou, et al, *Automatic Recognition System of Emotions Expressed through the Face Using Machine Learning: Application to Police Interrogation Simulation*, 2019 *3rd International Conference on Bio-engineering for Smart Technologies (BioSMART)*, 1-4.

benefits that such techniques can generate in the public safety sector, where, for example, the use of facial recognition can help in identifying suspects and finding missing persons. For these reasons, in recent years, we are witnessing the exponential spread (further driven by the pandemic emergency) of facial recognition and verification systems.

The positive effects of using these technologies do not stop at speeding up and making existing tasks more effective and efficient, but also take the form of enabling the performance of tasks and obtaining results previously not even imagined[18].

On the other hand, facial recognition raises significant ethical and legal questions[19].

The main critical issue with facial recognition is the risk that the use of this technology could seriously infringe on people's fundamental rights (such as the right to privacy)[20] and freedoms and degenerate, as has hap-

[18] As noted by M.M. Young, J.B. Bullock, J.D. Lecy, *Artificial Discretion as a Tool of Governance: A Framework for Understanding the Impact of Artificial Intelligence on Public Administration*, in *Perspectives on Public Management and Governance*, 2019, 1-13 "*This presents questions for scholars of governance as to how the governance tool of artificial discretion will affect the effectiveness, efficiency, and equity of governance, and for the manageability and legitimacy of the tool. But in cases of many emergent technologies, the challenge in predicting impact comes from new tasks that are made feasible, not the rationalization of existing tasks. For example, AI can be used to generate massive new data sets by automating the processing of images and sensors or by standardizing unstructured data such as social media posts or text*."

[19] On these issues see the monographic works of C. Grieco, *Intelligenza artificiale e tutela degli utenti nel diritto dell'Unione europea,* ES, Napoli, 2023; G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative.* ES, Napoli, 2021.

[20] On the issues that facial recognition techniques raise about respect for fundamental rights, *ex multis* M. O'Flaherty, *Facial Recognition Technology and Fundamental Rights*, in *European Data Protection Law Review (EDPL)*, vol. 6, no. 2, 2020, pp. 170-173; E.J. Kindt, (2013). *Privacy and Data Protection Issues of Biometric Applications, Dordrecht, Heidelberg*. Springer; N. Taylor, (2002), *State Surveillance and the Right to Privacy*, in *Surveillance & Society, 1*(1), 66-85. See also European Union Agency for Fundamental Rights (2019), *Facial recognition technology: Fundamental rights considerations in the context of law enforcement, November 21, 2019* available at https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law and P. Alston, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/74/493, October 11, 2019, available at https://undocs.org/A/74/493.

pened in some jurisdictions, into forms of mass surveillance[21] used to control the population and repress dissent[22].

Precisely in urban contexts, as mentioned above, there is great interest in this technology, the use of facial recognition in open places and even more so during demonstrations, can give rise to the so-called chilling effect, a 'chilling effect'[23], affecting an individual in such a way that, for fear of being watched, they choose to give up exercising their fundamental rights, from freedom of assembly to freedom of expression, even to the point of giving up, returning to the topic of smart cities, the right to experience the city for fear that their private sphere may be irreparably violated[24].

A second problem, also typical of other artificial intelligence systems, is the risk of mistakes and biases related to race or gender. The NIST

[21] Risk this made particularly real in the period of public health emergency due to the spread of Covid-19 (think of the use of facial recognition techniques to monitor the spread of the virus).

[22] Evident in this regard are the drifts that such tools can have, as witnessed by some examples from overseas: think of China's social scoring system or what occurred during the Hong Kong protests when authorities used facial recognition systems to identify protesters and repress freedom of expression and assembly. On which K.L.X. Wong and A.S. Dobson, *We're Just Data: Exploring China's Social Credit System in Relation to Digital Platform Ratings Cultures in Westernised Democracies*, in *Global Media and China*, 4(2), 220-232. See also Z. Doffman, *Hong kong exposes both sides of China's relentless facial recognition machine*. *Forbes*, August 26, 2019. On the topic see the chapter by Fulvio Costantino in this book.

[23] EU Commission, *White Paper on Artificial Intelligence - A European Approach to Excellence and Trustworthiness*, Brussels, 19.2.2020 COM(2020) 65 final. For an initial commentary S. Del Gatto, *Una regolazione europea dell'AI come veicolo di eccellenza e affidabilità. Gli obiettivi del Libro bianco della Commissione europea sull'intelligenza artificiale,* Osservatorio sullo Stato Digitale, IRPA, available online at https://www.irpa.eu/una-regolazione-europea-ai-delgatto/.

[24] On the risks that facial recognition could degenerate into forms of mass surveillance, last January the International network of civil liberties organizations, a network that brings together fifteen independent human rights organizations, published the report "In Focus", documenting thirteen cases of the use of facial recognition collected in as many states, from Hungary to India, South Africa and Russia. The report denounces how the spread of this tool ends up normalizing public surveillance practices, undermining not only privacy but also the rights to freedom of expression, protest and equality. On this topic, A. Mascolo, *Riconoscimento facciale e sorveglianza pubblica: una tecnologia in cerca di regolamentazione*, Osservatorio sullo Stato Digitale, available online at https://www.irpa.eu/riconoscimento-facciale-e-sorveglianza-pubblica-una-tecnologia-in-cerca-di-regolamentazione/.

Interagency 8280 report[25], dated December 2019, found that most facial recognition algorithms still have a high rate of false positives as well as, although to a lesser extent, false negatives, especially when referring to people from West and East Africa and East Asia. Algorithms developed in China show the same effect, but reversed, with low false positive rates on East Asian faces. In the United States, algorithms used by law enforcement reveal higher false positives in American Indians, with high rates in individuals of African descent[26]. In this regard, emblematic and well known was the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) case. Used in several U.S. jurisdictions, COMPAS was produced by a commercial company and designed to quantify the risk of recidivism of individuals undergoing criminal proceedings, to calculate the likelihood of commission of further offenses over the next two years, and to decide the type and *quantum* of punishment to be imposed. With reference to it, by analysing more than 10,000 criminal defendants in Broward County, Florida, and comparing their expected recidivism rates with the rate that actually occurred over a two-year period, some scholars have verified that black defendants were far more likely than white defendants to be wrongly adjudicated at higher risk of recidivism[27].

4. *Facial recognition governance attempts*

While waiting for the European legislator to take action, the matter of facial recognition has been the object of interesting acts of so-called

[25] Viewable at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[26] The reason often lies in the very design and initial testing of facial recognition systems. Indeed, in Western countries, experimentation, prior to actual use, takes place with "white" men with Western features. RF systems therefore are "untrained" to recognize individuals with different facial features thus generating, an error rate that then results, in de facto discrimination. On this topic, A. Najibi*, Racial discrimination in face recognition technology, science policy blog, Special Edition: Science policy and social justice*, October 24*,* 2020.

[27] The study is reported in J. Larson, S. Mattu, L. Kirchner, J. Angwin, *How We Analyzed the COMPAS Recidivism Algorithm*, May 23, 2016, available *online* at https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. See also S. Barocas, A.D. Selbst, *Big Data's Disparate Impact*, *California Law Review*, *June* 2016, Vol. 104, No. 3, p. 671 ff. and G. M. Haddad, *Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom,* in *Vanderbilt Journal of Entertainment and Technology Law, 23,* 891-918.

soft law: in 2021, the Advisory Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) adopted the "Guidelines on Facial Recognition" with the aim of outlining a set of measures that not only governments, but also facial recognition system developers, manufacturers, service providers and user organizations should apply to ensure that this technology does not undermine the human dignity, human rights, including the right to protection of personal data, and fundamental freedoms of any person[28].

Subsequently, in May 2022, the European Data Protection Board (EDPB) issued Guidelines on Facial Recognition by Law Enforcement[29]. In this document, the EDPB, while recognizing the undoubted benefits that such techniques can bring in the area of law enforcement, stressed that such tools must be used in strict compliance with the applicable legal framework and only in cases where the requirements of necessity and proportionality are met, as stipulated in Article 52(1) of the European Charter for Fundamental Rights. In providing its guidelines, the Board also considered that the use of facial recognition technologies in public settings, indiscriminately and in all cases where these technologies can determine the classification of individuals by sex, race, religion or political affiliation, should be prohibited, in the same way as technologies that can also determine a subject's state of mind from the physiognomy and physiology of the face. Unfortunately, the solutions indicated, while appreciable, suffer from the lack of legally binding effects inherent in acts of so-called "grey legislation".

Case law and privacy public independent authorities have also attempted to identify principles and criteria aimed at preventing the violation of the fundamental rights of those affected by the use of facial recognition technologies by public administrations.

Among the first cases to be decided by a judicial authority was that on the use of automatic facial recognition technology in public places by the Wales Police[30].

[28] The text is available *online* at https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html.

[29] The text is available online at https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.

[30] The lawsuit originated from an appeal brought by a civil rights activist who was unknowingly caught on camera in a shopping mall and, a second time, during an exhibition. According to the plaintiff, the Wales Police, on those occasions and, in general, during the testing phase of AFR technology, violated the *Data Protection Act*, the Human

After analysing the type of technology employed by the Wales Police and the concrete ways in which it was used, the lower courts dismissed the appeal and concluded that the authorities' actions were lawful[31]. According to the court, there was no conflict with paragraph 2 of Article 8 of the ECHR, according to which interference by a public authority is permissible only if it is provided for by law and constitutes a necessary measure for the protection of specific public interests (such as national security, or the protection of health)[32]. Furthermore, in the view of the

Rights Convention, and the *Equality Act*. In particular, the Police's processing of sensitive data (the biometric data collected by cameras in public places) was challenged as relating to ordinary people, not suspects, suspects or wanted persons, and as not strictly necessary for law enforcement purposes, as required by the regulations. The use of AFR technology would also violate Article 8 of the ECHR, which protects private and family life, as the power exercised by the Wales Police would lack a legal basis and consequently lack the requirements of "foreseeability, predictability, and hence of legality". Finally, the software used could result in erroneous *matches* due to the presence of *bias* and programming errors. On the matter see B. Davies, M. Innes, and A. Dawson, (2018), *An Evaluation of South Wales Police's use of Automated Facial Recognition*, Cardiff University, September 2018.

[31] See High Court of Justice Queen's Bench Division, Case No. CO/4085/2018, September 4, 2019 on which reference may be made to S. Del Gatto, *Quali regole per le nuove tecnologie di riconoscimento facciale? La Corte di giustizia di Cardiff si pronuncia per la legittimità dell'uso di tecniche di Automated Facial Recognition da parte della Polizia del Galles,* Osservatorio sullo Stato Digitale, IRPA, available online at https://www.irpa.eu/quali-regole-per-le-nuove-tecnologie-di-riconoscimento-facciale-la-corte-di-giustizia-di-cardiff-si-pronuncia-per-la-legittimita-delluso-di-tecniche-di-automated-facial-recognition-da-parte/.

[32] The use of facial recognition technology also, according to the judges, passes the so-called. *Bank Mellat test* under which an interference with rights under Article 8(1) ECHR can be justified only if the objective of the measure being pursued is sufficiently important to justify the restriction of a fundamental right; if there is a rational connection between the measure and the objective; if a less intrusive measure could have been used without unacceptably compromising the objective; and if, taking into account these aspects and the seriousness of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community. For the Court, in fact, AFR technology is aimed at crime prevention and its use in practice "struck a fair balance and was not disproportionate". Similar arguments were used by the British judges to reject the complaint regarding the alleged violation of personal data processing regulations. According to the judges, Section 35 of the *Data Protection Act* would be complied with because the AFR "*i*s strictly necessary to prevent and detect crime*"*. The court also found that the principles governing the actions of public authorities, contained in the Equality Act*,* were not violated: it was, in fact, affirmed that there is no valid reason to argue and prove that the accuracy of the *software* results may have been affected by factors such as gender or race.

judges regarding the necessary existence of a legal basis, there would exist "a clear and sufficient legal framework" represented by the primary law rules governing the powers and actions of the police, secondary legislative instruments, such as, for example, codes of conduct issued on the basis of primary law, and, ultimately, local policies adopted by the Wales Police[33]. The High Court of Justice thus concluded that the procedure followed by the police in using the data was "open and transparent" having, moreover, offered as an additional safeguard for the subjects filmed without their knowledge, the fact that, in the absence of a match between the captured image and a person on a checklist, all data corresponding to that image had been "immediately and automatically deleted".

The ruling[34] was reformed in August 2020. According to the Court of Appeal, the use of facial recognition technologies by the Wales Police was unlawful because it was not supported by an adequate legal basis and was adopted in violation of the Equality Act. The Court, in particular, censored what the judges called "fundamental deficiencies" in the legal framework for the use of facial recognition technology and in the policies that governed its use[35]. These deficiencies resulted in the police having "impermissibly wide" discretion[36], also producing negative consequences on the results of the DPIA conducted. According to the Court of Appeals, due to the legislative deficits, the DPIA, while correctly carried out by the police, would have led to the erroneous finding of compliance with Article 8 of the ECHR[37].

[33] As noted in the ruling, while these are already existing regulations, they can well be used for the regulation of the use of these new technologies and that applied as a whole they make the actions of the Police in the case "predictable and accessible" As noted by the Court, "[w]hat is important is to focus on the substance of the actions that use of AFR Locate entails, not simply that it involves a first-time deployment by SWP of an emerging technology. The fact that a technology is new does not mean that it is outside the scope of existing regulation, or that it is always necessary to create a bespoke legal framework for it".

[34] The conclusions of which immediately appeared to be criticized. See S. Del Gatto, *Quali regole per le nuove tecnologie di riconoscimento facciale?.,* cit., e Ead., *Potere algoritmico,* digital welfare state *e garanzie per gli amministrati.,* cit., 839, *sub* note 24.

[35] Royal Courts of Justice Strand, London, WC2A 2LL Date: 11/08/2020, available *online* at https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

[36] As noted by the English lower courts, "the current policies do not sufficiently set out the terms on which discretionary powers can be exercised by the police and for that reason do not have the necessary quality of law".

[37] The Court of Appeals has, specifically stated that: "The unavoidable consequence

The Court, then, upheld the last ground of appeal concerning compliance with Section 149 of the Equality Act of 2010, arguing that the NSW Police "never sought to ensure, either directly or through independent verification, that the software program had not caused unacceptable prejudice on grounds of race or sex". Finally, the Court concluded with the hope that "as AFR is a novel and controversial technology, all police forces that intend to use it in the future would wish to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias".

On the legality of the use of facial recognition, national privacy independent authorities have since ruled on several occasions.

In Italy, for example, the "Garante per la protezione dei dati personali (GPDP)" has rejected SARI Real Time, deeming it not in line with the standards imposed by the legislation on the matter. According to the Authority, SARI Real Time, insofar as it is installed in public places open to the public, would carry out large-scale automated processing that would extend even to those who are not included in the police watch-list, since the identification of the suspected person would require the biometric processing also of all other people who happen to be circulating in the monitored public space. This would result – in the view of the Authority – in an evolution of the very nature of surveillance activity, bringing about a shift "from targeted surveillance of certain individuals to the possibility of universal surveillance for the purpose of identifying certain individuals". It would, in essence, give rise to "a new surveillance model" that would introduce "*de facto*, a non-reversible change in the relationship between individual and authority"[38].

of these deficiencies is that, despite the DPIA's attempt to address the Article 8 issues, the DPIA failed to adequately assess the risks to the rights and freedoms of data subjects and failed to address the measures provided to address the risks arising from the deficiencies we found, as required by Article 64(3)(b) and (c) of the DPA 2018".

[38] Opinion, March 25, 2021, No. 127. Precisely because of the incisive interference with people's private lives – with the correlated risk of compression of certain individual and collective prerogatives of an essential nature, including the right to respect for personal life and freedom of expression – the Garante believes that such a device must be justified by an adequate regulatory basis that identifies the conditions of admissibility and limits. According to the GPDP, in order to be satisfactory, such a normative basis should take into account all the rights and freedoms involved and define the situations in which the use of such systems is possible, avoiding conferring "such a wide discretion that its use depends in practice on those who will be called upon to dispose of it, rather than on

Outside national borders, Canada's Federal Privacy Commission has observed that the use of facial recognition technologies by police for mass surveillance should be banned as overly intrusive to the privacy of individuals, also highlighting the need for legislation.

The privacy Commissions of Canada, France, the United Kingdom and Italy have, then, sanctioned the company *Clearview* for creating a database with billions of personal images, collected *online* without consent, in order to sell a biometric identification service to law enforcement agencies.

The issue of consent in relation to the use of facial recognition systems has also been the subject of other decisions. In Sweden, Datainspektionen (the National Data Protection Authority), fined a high school in Skellefteå for introducing a facial recognition system to check student attendance. Swedish legislation that implemented the GDPR includes an express prohibition on the processing of biometric data, such as those used in facial recognition. Although the school had stated that it had obtained the consent of the students, Datainspektionen found that in that specific case consent could not constitute an appropriate legal basis, given the position of subjugation in which the students find themselves in relation to the school (a public administration) and therefore decided to impose the sanction.

A similar case was decided by the Administrative Court of Marseille[39] where the local school office, after entering into a contract with the private company Cisco International Limited, had facial recognition cameras installed on students in a high school. Following an appeal filed by the parents' association, the Court censored the school office's decision, finding that there was a violation of the GDPR because the students could in no way provide free consent to the processing of their biometric data due

the enacted normative provision". Regulatory foundation considered by the *Privacy Authority* to be non-existent in national law to date, as no adequate legal basis for the processing of biometric data can be found either in Legislative Decree No. 51/2018 (which regulates the processing of personal data for the purpose of prevention, investigation, detection and prosecution of crimes) or in the Code of Criminal Procedure. On this topic, see A. Mascolo, *Riconoscimento facciale "in tempo reale": il Garante per la privacy boccia S.A.R.I. Real Time*, Osservatorio sullo Stato Digitale, IRPA, available *online* at https://www.irpa.eu/riconoscimento-facciale-in-tempo-reale-il-garante-per-la-privacy-boccia-s-a-r-i-real-time/.

[39] Tribunal Administratif de Marseille, February 3, 2020, No. 1901249, available online at https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf.

to the position of power in which the school authority holds over them. Such a surveillance system represented, according to the judges, an opt-out adherence, devoid of the possibility of withholding consent since the student who did not wish to be subjected to such processing would not be able to access the school building thus suffering an infringement of his or her right to education.

Referring to regulatory solutions, a significant watershed in the governance of facial recognition technologies was the entry into force in 2024 of the Artificial Intelligence Act[40] before which, Italy, choosing a solution of utmost caution, had banned the use of facial recognition systems *tout court*[41].

[40] Regulation (EU) 2024/1689 of the European Parliament and of the Council – June 13, 2024. The long gestation is partly due precisely to the tensions that the gradually proposed solutions on facial recognition have caused. In the long period between the proposal for a Regulation put forward by the Commission in 2021 and its final approval, positions on facial recognition technologies have, in fact, changed several times due to the attempt to hold together the different positions on the subject brought forward by individual states and European institutions. After an initial move away from the position of total closure immediately expressed by the European Parliament (on October 6, 2021, the European Parliament had voted by a majority vote a resolution calling on the European Commission to ban, by a general regulatory act, facial recognition as a general prevention tool throughout the European Union. See https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_IT.pdf), subsequent versions of the *AI Act* appeared to be more cautious until the final version in which we see a substantial compromise such that, it was said, it bans facial recognition technologies, but with some openings explainable by the need to consider the position of some member states opposed to the full ouster of this technique.

[41] See Decree Law Oct. 8, 2021, No. 139 "Urgent provisions for access to cultural, sports and recreational activities, as well as for the organization of public administrations and in the field of personal data protection" aimed at introducing provisions on the management of the pandemic emergency from Covid 19. The deadline initially set for Dec. 31, 2021 was first moved to Dec. 31, 2023 and lastly postponed to the end of December 2025 by Article 8 of Decree Law "Public Entities," May 10, No. 51. The prohibition therein is not, however, absolute: processing carried out by the competent authorities for the purpose of preventing and suppressing crimes or enforcing criminal sanctions is excluded, provided that there is a favourable opinion from the Data Protection Authority. The opinion is not, however, necessary where the processing is carried out by the judicial authority in the exercise of judicial functions as well as judicial functions of the public prosecutor. The solution adopted by the Italian legislature appears inadequate to deal with the new challenges posed by the use of facial recognition, particularly by public authorities, and on closer inspection does not meet either the expectations of those in favour of the use of these technologies in public places or those open to the public, or those against it. The rule banning facial recognition, specifically, appears short-sighted, not very courageous, and not decisive. Timid and short-sighted because it takes into ac-

The AI Act, on the contrary, adopts a compromise solution that bans facial recognition technologies but with some openings due to the position expressed by some member states opposed to the full ouster of this technology: in accordance with the risk-based approach underlying the entire Regulation, real time facial recognition systems, as qualified high-risk artificial intelligence systems, are banned except for law enforcement reasons and under certain prerequisites and limitations[42].

5. *Conclusions*

How does this reflect on the nature of public power and the relationship between "authority" and "freedom" and between public administrations that use facial recognition in the exercise of their functions and the recipients of measures taken? Does the use of these technologies by public power result in a significant change in the existing model, starting with the Italian constitutional model, of the relationship between public administration and citizens?

In our system, in the pursuit of the interests of public safety and public order, citizens' freedoms represent a logical and legal *prius*, from

count neither inevitable technological progress nor the actual needs of citizens to be able to take advantage of the benefits made available by facial recognition technologies. It is unhelpful from a fundamental rights protection perspective because the ban introduced is subject to very broad limits. See S. Del Gatto, *Facial Recognition in Italy: legal problems and perspective, in European Review of Digital Administration & Law-ERDAL*, 2025, *forthcoming.*

[42] Art. 5(2). Art. 5(d) prohibits the use of *real time* biometric identification systems in spaces open to the public for law enforcement purposes, unless strictly necessary for the targeted search of potential victims of criminal actions, such as missing children, for the prevention of a specific, substantial and imminent danger to a person's life or safety or a terrorist attack, or, finally, for the detection, location or incrimination of a person suspected of crimes under Art. 2(2) of Council Framework Decision 2002/584 for which the member state concerned provides for a prison sentence of three years or more. Where facial recognition is intended to achieve these objectives, the draft regulation stipulates that the authority must consider the concrete situation, and in particular the severity, likelihood, and extent of the harm that would be caused by not using the identification system, and the consequences that the use of the identification system might have for the rights and freedoms of the persons involved. The individual use of facial recognition requires in any case, a prior authorization issued by the judicial authority or an independent administrative authority following a reasoned application and in accordance with national law.

which the limits to the exercise of power are set[43]. The system outlined by the Italian Constitution, places fundamental freedoms at the centre from which to conform and limit authoritative power. This adopted angle of view is emblematic of a broader choice in favour of a precise way of understanding the relationship between public powers and the citizen, even when it is the so-called *puissance publique*[44] that is exercised.

Compared to this model, the use of facial recognition, particularly by police forces or municipalities with a surveillance function in cities, seems to lead, by contrast, to a reversal of this setup with the risk of again placing some fundamental freedoms of individuals in a subordinate position.

Indeed, what was observed in the preceding paragraphs (§§ 3 and 4) offers a not very reassuring picture of algorithmic administrative power when it makes use of such intrusive technologies as facial recognition. A power that is opaque, less accountable, that presents accentuated characters of authoritativeness and unilateralism, and that indicates a clear imbalance in favour of the public administrations with reference to the relationship between "authority" and "freedom"[45].

This is aggravated by the increasingly broad delegation of decision-making to third parties (in some cases private parties) with respect to the public administration, to whom the latter entrusts the processing of the software[46] (not always fully transparent or knowable to the public

[43] See Articles 13, c. 3, 16, c. 1, 17, c. 3 and 21, c. 4 Const. On the subject, G. Corso, *L'ordine pubblico,* Bologna, Il Mulino, 1979, *passim.*

[44] A. Pubusa, *Riflessioni sulla pubblica amministrazione rileggendo la Costituzione,* in *Studi in onore di Feliciano Benvenuti*, VI, Mucchi Editore, 1996, pp. 1471 ss.; AA.VV., *Valori costituzionali e pubblica amministrazione*, 1993, *passim*; V. Allegretti, *Amministrazione pubblica e Costituzione*, Padova, Cedam, 1996, *passim.*

[45] Garante per la protezione dei dati personali, Opinion March 25, 2021 No. 127. According to the Garante, *Real time* facial recognition realizes large-scale automated processing that can affect, among others, those who are present at political and social events, which are not the subject of 'attention' by the police forces.

[46] This delegation can also be direct, as, for example, has happened in Australia, where the government has outsourced the power to issue certain benefits under *welfare* policies, without, among other things, complying with public evidence procedures. On the Australian case of the debit card (whereby benefits are loaded onto that card, which, however, cannot be used for certain purchases, e.g., alcohol or gambling, or in certain establishments) S. Tilley, *In the Name of 'Digital Inclusion': The true cost of the automation and privatization of Australia's social security system*, in *Social Alternatives*, vol. 39, 1, 2020, pp. 28 ff. The points criticized are compulsoriness, lack of consent, and decision-making based only on the use of data. According to the Author, the government is abdicating its responsibility for what citizens' needs are to be met, putting the choice back to the algorithm. This form of exercising power would also alter the very position of

authority) *de facto* outsourcing the care of the public interest. This generates important questions: the imputability[47] of the algorithmic administrative choice, its explicability and the responsibility[48] with regard to the decisions made. With respect to which, moreover, there is also the fear of a risk of flattening of the decision maker to the findings of the machine, which goes far beyond the subordination of the administrative decision to the technique[49].

In these cases, there is a risky "reintermediation" of public authority[50], realizing the eventuality whereby in discretionary activities the use of new technologies determines an "unconscious constraint" such that the decision is "not simply anticipated, but replaced by technique"[51].

The question then arises as to whether in the face of such risks and problems the choice initially followed by the Italian legislature which, it has been said, has banned the use of facial recognition systems[52] (as in many other non-EU legal systems[53]) should be endorsed, or, motivated by

welfare recipients, whom the A. defines as "actors necessarily conforming to the market". In this vein also M. Langford*, Taming the Digital Leviathan: Automated Decision-Making and International Human Rights*, AJIL Unbound, 114, p. 141-146 according to which "*The digital welfare state, unwittingly or not, provided a useful "neutral" cover for long-standing neoliberal policies that challenged the right to social security, whether by reducing welfare budgets, narrowing the beneficiary pool, or enhancing sanctions*".

[47] M.C. Cavallaro, *Imputazione e responsabilità delle decisioni automatizzate*, in *European Review of Digital Administration & Law – Erdal*, 2020, pp. 69 ff.

[48] See on this topic the interesting reflections on the increase of freedom at the expense of responsibility in the "digital society" carried out by L. Violante, *Diritto e potere nell'era digitale. Cybersociety, cybercommunity, cyberstate, cyberspace: tredici tesi*, in *BioLaw Journal,* 2022, pp. 145 ff. On these issues already S. Del Gatto*, Potere algoritmico.,* cit., pp. 829 ff.

[49] S. Stacca, *Potere algoritmico. Profili organizzativi del rapporto tra amministrazione e automazione,* in *Dir. pubbl.,* 2024, pp. 365 ff.

[50] That is, the risk noted is that we are not simply witnessing the "cancellation of mediators" but a "discreet replacement of them". Thus L. Violante*, Diritto e potere.,* cit., 145 ff.

[51] The reference is again to S. Stacca*, Potere algoritmico.,* cit., pp. 365. See already A. Cassatella*, La discrezionalità amministrativa nell'età digitale*, in Scritti per F.G. Scoca, Napoli, E.S., 2020, pp. 681 ff. as also cited by S. Stacca.

[52] *See supra sub* note 20.

[53] In the United States, for example, some states have decided to ban facial recognition *tout court* or to introduce specific sectoral bans, for example, in schools or public housing. Facial recognition is banned, with specific reference to police functions, in Boston, San Francisco, Minneapolis, Oakland, and California. In the State of Maine, the law prohibits state, county, and municipal departments, employees, and officials from using or possessing facial recognition technology or entering into an agreement with a third

the positive benefits that such technology can determine in the performance of certain public functions and services[54], whether it would not be preferable to investigate the possibility of finding appropriate correctives capable of restoring a fair balance between public power and individual rights and freedoms when using facial recognition systems.

However, the solutions reviewed above do not seem satisfactory.

At the regulatory level, the AI Act leaves (too) wide discretion to member states on the law enforcement assumptions that allow the use of this technology. There is also evidence of excessive vagueness, too much leeway given to member states to implement the exception to the ban on remote facial recognition systems for law enforcement purposes, and a lack of adequate public oversight of the proposed standardization and self-assessment processes[55].

Insufficient, too, seem to be the safeguards, identified by case law and privacy authorities and linked to the granting of consent to the processing of biometric data: it is doubtful that consent can ever be considered freely given and therefore effective when there is such an imbalance of positions as that between public administration and the administered. "Voluntary" subjection to a surveillance system that makes use of facial recognition by a public authority translates in fact into opt-out adherence, lacking the real possibility for the individual to deny his or her consent[56].

party to obtain, access, or use facial recognition technology in most public areas, including schools, and for surveillance purposes. There is also a strict regulatory framework as to the specific ways in which law enforcement agencies can exploit the relevant technology for crime suppression and investigation.

[54] Also having in mind the reconstruction of Feliciano Benvenuti who observed that the justification of power is instrumentality to social utility and general interest. The duties of security police are directed to the service of the community and citizens by providing to enable individuals to live peacefully in the community and to act in it for the manifestation of their individuality and the satisfaction of their interests F. Benvenuti, *Appunti di diritto amministrativo*, *Parte generale*, cit., 183.

[55] The *summa divisio* made in the AI Act between low-risk and high-risk biometric systems does not seem, in general, entirely convincing, and the choice to give private companies themselves the task of assessing the compliance of the software produced with security and quality standards without public intervention, for example by an independent authority established ad hoc, raises strong concerns C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento in materia di intelligenza artificiale*, in *BioLaw Journal*, 3/2021; G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. informaz. e informat.,* 2022, pp. 303 ff.

[56] Significant in this regard are some cases that occurred in Sweden and France. With

Not very decisive is also the guarantee indicated by the Italian judge and now transposed into the new Italian law on artificial intelligence [57]of the so-called "reservation of humanity" or non-exclusivity of the algorithmic decision[58]. The reasons inherent in the criticality of the corrective offered by the so-called human in the loop lie in the very character of the algorithms used[59] whose functioning can be difficult to understand even for the programmers themselves[60]. Consequently, a serious problem of

reference to the latter, see the decision of the *Tribunal Administratif de Marseille*, Feb. 3, 2020, No. 1901249, available *online* at https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf.

[57] Article 14, L. n° 132/2025 on 'Use of artificial intelligence in public administration' establishes that public administrations shall use artificial intelligence for the purpose of increasing the efficiency of their activities, reducing the time required to complete procedures, and increasing the quality and quantity of services provided to citizens and businesses, ensuring that interested parties are aware of how it works and that its use is traceable. The use of artificial intelligence can only be allowed for an instrumental and supportive capacity to the decision-making process, respecting the autonomy and decision-making power of the person who, according to the provision referred to, remains solely responsible for the measures and procedures in which artificial intelligence has been used.

[58] Human involvement, so-called human in the loop, while not sufficient is considered a necessary element for the legitimacy of the use of facial recognition software by public authorities. For a definition of human in the loop, see the Ethical Guidelines for Trustworthy Artificial Intelligence, developed by the High-Level Panel on Artificial Intelligence, published in April 2019 and laid the foundation first for the AI White Paper and then for the *AI Act*. On this topic extensively G. Gallone, *Riserva di umanità e funzioni amministrative*, Padova, Cedam, 2023, *passim.* Also interesting is the analysis from a sociological perspective by B. Marchetti, *La garanzia dello Human in the loop alla prova della decisione amministrativa algoritmica*, in *Biolaw Journal*, 2021, pp. 367 ff.

[59] Reference is made to so-called *machine learning* algorithms and algorithms that generate predictive and decision-making *output* from their learning system. These are, in fact, algorithms that transform the huge amount of incoming data (even heterogeneous to each other and unstructured), into new information, generating correlations and predictive models not on the basis of a deductive logical process, but based on probabilities. In other words, the interweaving of data by these systems is able to learn by other means, what is not known directly. The prediction mechanism underlying machine learning can, however, realize discriminatory and stigmatizing effects: relying on time series, they work out a trend on which they make a prognostic judgment that tends to "freeze" pre-existing situations, with the consequence of perpetuating and exacerbating inequalities, regardless of the initial will of those of the programmer.

[60] G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza,* in *Pol. dir.*, 2019, p. 217; F.Z. Borgesius (ed.), *Discrimination, Artificial Intelligence, and Algorithmic Decision Making*, Council of Europe, Strasbourg,

transparency and comprehensibility of the assumptions of the "algorithmic decision" arises[61]. When the basis of the decision is an output produced by artificial intelligence software, as in the case of facial recognition, transparency, even in the strengthened version affirmed by the Council of State[62], risks offering only "a snapshot" of the functionality of the system[63], which favours "vision" to "understanding", significantly limiting the benefits attributable to its operation[64].

2018; Federal Trade Commission, *Data Brokers. A Call for Transparency and Accountability, Washington*, 2014, pp. 10 ff.; S. Del Gatto, *Potere algoritmico.,* cit., pp. 829 ff.

[61] On the black box character algorithms see F. Pasquale, *The black box society,* Harvard University Press, 2015 in which the A. points to a number of examples to support the thesis that while companies and institutions are increasingly subject to the "logic of secrecy," people's lives are increasingly transparent and open. Also on the subject is I.M. Delgado, *Automation, artificial intelligence and public administration: old conceptual categories for new problems?, Institutions of Federalism*, 3, 2019, pp. 643 ff. As noted by the A. with reference to self-learning systems, "[t]*he machine learning* possesses three well-known characteristics that distinguish it from other types of techniques: it is based on the use of algorithms that learn autonomously, these algorithms are *black box* in nature, and the system has the ability to produce results that could potentially exceed human prediction. The first relates to "explainability": if information is transformed into predictions through a *black box* in a way that is not fully knowable, how do we motivate the measure? […]". On the problem of transparency in AI systems and possible solutions also in light of the principles of the new Public Contracts Code, see E. Carloni, *Transparency within the artificial administration, principles, paths, perspectives and problems,* in *Italian Journal of Public Law*, 2024, pp. 8 ff.

[62] As noted by the administrative judge, "the use of computerized procedures cannot be a reason to circumvent the principles that conform our system and regulate the conduct of administrative activity". Cons. St., VI, Dec. 13, 2019, No. 8472, § 10. See also *Décision* n° 2018-765 DC, June 12, 2018 of the *Conseil Constitutionnel*, which recognized the legitimacy of the use of algorithms in administrative proceedings, provided that the full intelligibility of the algorithmic procedure is ensured and-if the decision is based on or concerns sensitive data-that the final decision is not fully automated. The importance of having an adequate discipline of algorithmic procedure has also been highlighted by C. Harlow, R. Rawlings*, Proceduralism and Automation: Challenges to the Values of Administrative Law*, in E. Fisher, J. King, A. Young (eds.), *The Foundations and Future of Public Law* (in honor of Paul Craig), LSE Legal Studies Working Paper No. 3/2019; J. Cobbe, *Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making*, in *Legal Studies*, 39 (4).

[63] This is especially true for adaptive systems that learn as the amount and types of data they draw on increases, and for platforms with mobile interfaces, settings, features, and number of users.

[64] Doubts as to whether transparency in decisions using algorithms can be guaranteed have been raised by D. Runciman, *How Democracy Ends*, UK, 2018. According to the A., algorithms in decisions would prevent a balanced system of checks and balances and

In addition to transparency, the enhancement of two other typical principles of administrative law then appears important: the principle of legality and the principle of proportionality. While respecting the principle of legality to be understood, as suggested by the Italian GPDP, in a strict way and to be scrutinized in "qualitative" terms, the use of facial recognition by the public administration should always be based on an *ad hoc* legal basis. Therefore, a generic provision allowing the public administration to use such technologies cannot be said to be sufficient, but it is necessary, because of the intrusiveness and characteristics of such tools, the existence of a detailed discipline[65] that does not merely attribute the power, leaving the administration free in the choice of means to exercise it, but that indicates with a high degree of detail the prerequisites for its exercise and formulates the limits to the exercise of discretion[66]. In the

offer only unidirectional transparency-that is, that of the administration that makes use of the algorithm-about the data subject. On the risks of achieving transparency that is "fuzzy" or in other respects harmful, P.B. de Laat, *Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?*, *Philos. Technol.,* 31, 2018, p. 525.

[65] This is also the direction taken by the Personal Data Protection Authority, which has deemed the SARI *real time* tool illegitimate because it is used in the absence of an adequate legal basis. According to what the Data Protection Authority said, the implementing decree of the Personal Data Protection Code regarding the processing of data carried out for public security purposes by police organs, offices and commands cannot be considered an adequate and sufficient legal basis because it lacks the degree of detail necessary to meet the need for predictability that is fundamental when police use real-time facial recognition technologies. In the decree referred to by the Guarantor there is in fact, only a specific regulation for the processing of data collected through video surveillance and photographic, audio and video recording systems, which, however, as noted by the Guarantor, are "ontologically different systems from those for biometric data processing". The importance of a regulatory prerequisite indicating in detail assumptions and limits was recently affirmed with reference to facial recognition technologies by the EDU Court, which affirmed the fundamental importance-when using such technologies-of having sufficiently detailed rules governing the scope and application of the measures taken and, at the same time, strong safeguards against the well-founded risk of possible abuse. See ECHR, III, July 4, 2023, Case 11519/20, *Glukhin v. Russia.*

[66] One of the first cases of police use of facial recognition technologies to come under judicial review is that of the Wales Police. The Court of Appeal has overturned the decision of the lower courts, which had declared the actions of the Welsh Police to be lawful. According to the Royal Courts of Justice, the use of AFR technology, violates Article 8 of the ECHR, which protects private and family life because the power exercised by the Welsh Police appears to lack a specific and sufficiently detailed legal basis and consequently such power would lack the requirements of "foreseeability, predictability, and hence of legality". The police who had made use of such technologies would, in the

narrow cases permitted, moreover, the use of facial recognition should always be preceded by a scrutiny of compliance with the principle of proportionality. The mere, albeit essential, presence of a public interest that, screened by the legislature, allows the use of a video surveillance system with facial recognition software is, in fact, insufficient if not accompanied by a judgment on the proportionality of the measure, in particular, on its tolerability (also called "proportionality in the strict sense"). This element (which together with those of suitability and necessity concurs to fill with content the principle of proportionality), often little investigated in the judgments of the administrative judge, in this case should have instead, a central role.

However, in the face of the rapid evolution of new technologies even these correctives may not be sufficient making it necessary to identify an insurmountable limit, an intangible core of rights that benefits from an absolute protection against intrusion by public administration[67], in order to ensure a fair relationship between "authority" and "freedom" put at risk by the use of some technologies considered too intrusive.

Court's view, have enjoyed an "*impermissibly wide*" discretion due to the lack of an adequate legal basis. Royal Courts of Justice Strand, London, WC2A 2LL, August 11, 2020, available *online* at https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf. On the matter see B. Davies, M. Innes and A. Dawson, *An Evaluation of South Wales Police's use of Automated Facial Recognition*, Cardiff University, September 2018.

[67] The existence of intangible core of private life (*Kernbereich privater Lebensgestaltung*) as an insurmountable limit in the face of certain public interference was affirmed by the German Constitutional Court in 2016, which declared the illegality of state-of-the-art covert surveillance tools used in the context of counterterrorism. *Bundesverfassungsgericht*, April 20, 2016, 1 BvR 966/09 and 1 BvR 1140/09, at www.bundesverfassungsgericht.de. According to the court, the more substantial the measure's interference in an individual's private life, the more stringent the legal requirements for its implementation must be. For the judges, a relationship of direct proportionality between the degree of intrusiveness of the measure and the level of intensity of the legal safeguards must, in essence, be affirmed. See paras 105 and 108 of the judgment.

Stefano Billi*

RICONOSCIMENTO FACCIALE E DIRITTI FONDAMENTALI: CONSIDERAZIONI DI DIRITTO PROCESSUALE PENALE PER IL DECIMO CONVEGNO ANNUALE "ICON"[1].

Sommario: 1. Premesse introduttive. – 2. Una breve ricognizione sui sistemi di riconoscimento facciale. – 3. Le criticità dei sistemi di riconoscimento facciale con riguardo al processo penale; problemi di una disciplina normativa ancora "incompiuta". – 4. Conclusioni. – 5. Bibliografia.

1. *Premesse introduttive*

Non può passare inosservato come la giustizia penale, insieme a numerosi altri contesti sociali, sia chiamata a confrontarsi con l'avvento di nuovi strumenti tecnologici – siano essi concepibili in guisa di dispositivi elettronici o di programmi computazionali – il cui utilizzo è ormai indispensabile nel compimento delle quotidiane attività da espletare in sede processuale, anche nell'ottica di un ammodernamento ed un efficientamento delle prassi da seguire. Ad esempio, basti pensare come, attualmente, anche il rito penale sia orientato verso un'inesorabile transizione digitale e telematica[2], all'interno della quale tutte le parti coinvolte – sia-

* Avvocato presso il foro di Viterbo e assegnista di ricerca presso l'Università di Macerata)

[1] Il presente contributo si colloca nell'ambito del progetto di ricerca PRIN 2022 sul tema "Nuove tecnologie, dati biometrici e procedimenti penali" – CUP: D53D23007120006 (Finanziato dall'Unione europea – Next Generation EU – missione 4, componente 2, investimento 1.1).

[2] Tra gli aspetti maggiormente rilevanti della c.d. "riforma Cartabia" (ossia, della Legge 27 settembre 2021, n. 134) occorre tenere in considerazione proprio la c.d. *digital transformation* del processo penale. Come riscontrabile nella relazione illustrativa al decreto di attuazione della predetta "riforma Cartabia" (ovvero il decreto legislativo 10 ottobre 2022, n. 150), «il legislatore delegante ha inteso delineare un unico e organico contesto normativo di riferimento, idoneo ad istituire un ambiente (o ecosistema) digitale per il procedimento penale, ovvero un insieme (…) di previsioni normative che siano tali da favorire la transizione digitale» (vedasi, in merito a questo precipuo aspetto, Ufficio Legislativo del Ministero della Giustizia, *Relazione illustrativa al decreto legislativo 10 ottobre 2022, n. 150: «Attuazione della legge 27 settembre 2021, n. 134, recante delega al*

no esse pubbliche o private – debbono ricorrere alla fruizione di apparati (per lo più di natura informatica) per compiere non solo i tradizionali tipi di attività processuali (come, in ipotesi, la redazione di documenti, che da una versione analogica oggigiorno avviene attraverso una stesura in formato digitale), ma anche nuove attività che, in passato, non erano nemmeno ipotizzabili (come la trasmissione telematica di documenti difensivi mediante specifiche piattaforme *online* quali, ad esempio, il "Portale deposito atti penali"[3], che funge da modalità succedanea alla consegna *brevi manu* degli incartamenti presso le cancellerie o le segreterie competenti, ovvero la possibilità di celebrare l'udienza attraverso videocollegamenti o, ancora, l'informatizzazione nella gestione del processo penale telematico avviata attraverso l'ormai noto applicativo denominato "App")[4].

Governo per l'efficienza del processo penale, nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari», in *Gazzetta Ufficiale* (supplemento straordinario n. 5 alla Serie generale n. 245 del giorno 19 ottobre 2022), Roma, 2022, p. 185, Istituto Poligrafico e Zecca Dello Stato, consultato – da ultimo – in data 06 dicembre 2024 alla pagina *web* https://www.gazzettaufficiale.it/do/gazzetta/serie_generale/0/pdfPaginato?dataPubblicazioneGazzetta=20221019&numeroGazzetta=245&tipoSerie=SG&tipoSupplemento=SS&numeroSupplemento=5&progressivo=0&numPagina=1&edizione=0&elenco30giorni=true). Una siffatta transizione digitale del processo penale è concepita dal Legislatore come un insostituibile veicolo di efficientamento del processo e della giustizia penale, in vista della piena attuazione dei principi costituzionali, convenzionali e dell'U.E. nonché del raggiungimento degli obiettivi del P.N.R.R. (vedasi, ancora, la predetta *Relazione illustrativa*, p. 182).

[3] Oltre al "Portale deposito atti penali", la transizione verso un "rito" penale telematico si avvale dell'intervento anche di altri strumenti come – a titolo esemplificativo e non esaustivo – il "Sistema Notifiche Penali Telematiche" (c.d. "S.N.T."), oppure l'applicativo c.d. T.I.A.P. (cioè, il "trattamento informatico degli atti penali") o, ancora, il "Portale NDR" (ossia il "Portale delle Notizie di Reato") o, inoltre, l'applicativo c.d. "APP" relativo alla gestione del processo penale telematico.

[4] La transizione del processo penale ha, indubbiamente, subito un'accelerazione temporale anche a causa della passata emergenza pandemica (esplosa nell'anno 2020), allorquando si delineò l'impellente esigenza che il compimento di numerose attività processuali – come, ad esempio, il deposito di atti e documenti, le comunicazioni e le notificazioni – avvenissero in modalità telematica (vedasi, sul punto, P. Bronzo, *Delega al governo per l'efficienza del processo penale e disposizioni per la celere definizione dei procedimenti giudiziari pendenti presso le corti d'appello*, in *Cassazione penale*, Milano, 2021, fasc. 10, p. 3278, Giuffrè Francis Lefebvre). È, infatti, innegabile riconoscere come il procedimento penale telematico, durante la pandemia, si sia «espanso ben oltre quanto sarebbe stato immaginabile in un periodo non emergenziale» (*cfr*. V. Bove, R. Patscot, *Processo penale telematico: dalla fase emergenziale alla digital transformation della giustizia penale*, in *Ius*, Milano, 06 Aprile 2021, p. 19, Giuffrè Francis Lefebvre). Sul punto, è possibile

In questo siffatto scenario di avvento tecnologico – che si palesa, già di per sé, come rivoluzionario, tenendo in considerazione come per decenni l'amministrazione della giustizia penale abbia manifestato un'atavica ritrosia all'innovazione informatica[5] – un nuovo elemento di novità complica ulteriormente il tema della transizione digitale: la possibilità di applicare la cosiddetta intelligenza artificiale[6] al diritto e, più in partico-

richiamare, altresì, quanto evidenziato da L. Giordano, *La giurisprudenza e la digital transformation del processo penale*, in *Sistema penale*, Associazione "Progetto Giustizia Penale", Milano, 08 Gennaio 2024, p. 2, consultato – da ultimo – in data 09 dicembre 2024 alla pagina *web* https://www.sistemapenale.it/pdf_contenuti/1704142876_giordano-digital-transformation.pdf: secondo questo Autore, «la pandemia, infatti, ha determinato una forte spinta all'impiego dell'informatica nel processo penale, che si è concretizzata in un più ampio utilizzo degli strumenti telematici per le notificazioni, nella possibilità del deposito degli atti con modalità tecnologiche e nella sperimentazione della trattazione del procedimento e della deliberazione collegiale a distanza».

[5] Il procedimento penale, infatti, anche in considerazione della sua «carica rituale (o ritualistica, se si vuole), si mostra meno recettivo di altri contesti al recepimento dei frutti del progresso tecnologico» (S. Quattrocolo, *Le nuove tecnologie e il futuro del diritto pubblico; introduzione*, in *La legislazione penale*, Dipartimento di Giurisprudenza dell'Università degli Studi di Torino, Torino, 16 ottobre 2020, p. 1, consultato – da ultimo – in data 08 dicembre 2024 alla pagina *web* https://www.lalegislazionepenale.eu/wp-content/uploads/2020/10/Introduzione-Quattrocolo-finale.pdf). La stessa Autrice sottolinea, peraltro, come «i riflessi dei più profondi mutamenti della società si proiettano sulla giustizia penale con un significativo ritardo, ovvero quando quei mutamenti possono considerarsi ormai sedimentati nel sentire comune» (S. Quattrocolo, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *Media Laws - Rivista di Diritto dei Media*, Università "L. Bocconi", Milano, 2020, fasc. 3, p. 122).

[6] Si potrebbe definire "intelligenza artificiale" l'abilità di una macchina (o, più precisamente, come la capacità di un sistema informatico) di interpretare autonomamente e correttamente dati esterni – imparando da quest'ultimi – e quindi utilizzarli al fine di raggiungere specifici obiettivi e compiti, attraverso un adattamento flessibile. L'utilizzo del modo verbale condizionale è qui tuttavia d'obbligo giacché – come puntualizzato in C. Bartneck e al., *An Introduction to Ethics in Robotics and AI*, Switzerland, 2021, p. 8, Springer – la definizione stessa di intelligenza artificiale è volatile ed è cambiata nel tempo. Lo stesso concetto di intelligenza artificiale è, peraltro, intrinsecamente vago, in considerazione della oggettiva difficoltà di delineare, in relazione a tale argomento – una nozione unica di raziocinio riferibile sia all'essere umano che all'apparato "macchina" (*cfr.* High-Level Expert Group on Artificial Intelligence, *A definition of AI: main capabilities and disciplines*, Brussels, 8 April 2019, p. 1, European Commission, consultato – da ultimo – in data 08 dicembre 2024 alla pagina *web* https://digital-strategy.ec.europa.eu/it/node/2226). Sul punto, prezioso è il contributo di L. Portinale, *Intelligenza Artificiale: storia, progressi e sviluppi tra speranze e timori*, in *Media Laws - Rivista di Diritto dei Media*, Università "L. Bocconi", Milano, 2021, fasc. 3, p. 14, in virtù del quale è possibile approfondire come, allorquando si tratti del tema dell'intelligenza artificiale, sia necessario affrontare anche i concetti di *machine learning* (c.d. "m.l.", o apprendimento automa-

lare, anche alla scienza processual penalistica[7]. L'intelligenza artificiale, infatti, può divenire un utile strumento di cui poter fruire in tutte le fasi del procedimento penale – già dal suo avvio (all'interno delle indagini preliminari) sino a tutto l'arco dibattimentale, passando finanche per l'eventuale esecuzione della pena – dispiegando i suoi ambiti applicativi in favore non solo delle autorità requirenti (si pensi, ad esempio, al campo dell'identificazione e all'uso di sistemi di riconoscimento facciale[8], di cui si tratterà più approfonditamente qui appresso), ma anche degli organi giudicanti (basti annoverare, sul punto, i discussi campi d'azione della giustizia predittiva[9] o delle *digital evidence* e *automated evidence*[10]). Ed

tico) e *deep learning* (c.d. "apprendimento profondo"). Secondo tale Autore, il *machine learning* concerne la precipua capacità «di sviluppare sistemi artificiali (che possiamo chiamare agenti) imparando dalle capacità acquisite tramite l'esperienza» (*supra*); viceversa, con l'espressione intelligenza artificiale ci si riferisce ad un concetto più ampio, riguardante «*la costruzione di agenti intelligenti che, una volta apprese le informazioni necessarie (sia dai dati sia perché fornite esternamente in qualche altra forma), sfruttano quest'ultime per svolgere specifici compiti, i quali normalmente richiedono una qualche forma di intelligenza per essere portati a termine*».

[7] Non deve sorprendere come anche il diritto processuale penale entri in relazione con il tema dell'intelligenza artificiale, poiché quest'ultima può rappresentare un notevole strumento di ausilio pure in ambito giuridico, allo scopo di rendere il diritto più comprensibile, gestibile, utile, accessibile e soprattutto prevedibile (cfr. H. Surden, *Artificial Intelligence and Law: An Overview*, in *Georgia State University Law Review*, Atlanta, 2019, vol. 35, fasc. 4, p. 1326-1327, Georgia State University).

[8] Cfr. P. Contardo e al., *Deep learning for law enforcement: a survey about three application domains*, in E. Xhina (a cura di), *Proceedings of the 4th International Conference on Recent Trends and Applications in Computer Science and Information Technology*, Tirana, 2021, vol. 2872, p. 1-2, CEUR Workshop Proceedings, consultato – da ultimo – in data 06 dicembre 2024 alla pagina *web* https://ceur-ws.org/Vol-2872/.

[9] A primo acchito, l'espressione "giustizia predittiva" può essere definita come «un sistema che consente di prevedere il possibile esito di una controversia sulla base delle precedenti soluzioni date a casi analoghi o simili» (C. Castelli, *Giustizia predittiva*, in *Questione Giustizia online*, Roma, 08 febbraio 2022, Associazione Magistratura Democratica, consultato – da ultimo – in data 08 dicembre 2024 alla pagina *web* https://www.questionegiustizia.it/articolo/giustizia-predittiva). Tuttavia, una disamina più attenta dell'argomento deve suggerire come la possibilità di applicare tecnologie ad ambiti di tipo giuridico, giurisprudenziale o giudiziario non deve indurre nell'errore per cui ci si possa illudere che un algoritmo possa «predire con esattezza puntuale il dispositivo di una sentenza»: al contrario, la predizione di cui trattasi sarà invece utile per «individuare l'orientamento del ragionamento del giudice» (C. Castelli, D. Piana, *Giustizia predittiva. La qualità della giustizia in due tempi*, in *Questione Giustizia*, Roma, 2018, fasc. 4, p. 154, Associazione Magistratura Democratica).

[10] Tra le aree del sistema processuale penale maggiormente interessate dall'impatto dell'evoluzione tecnologica non si può, infatti, non considerare anche quella delle prove:

anche se, oggigiorno, l'intelligenza artificiale non ha ancora espresso – in termini di incidenza sul processo penale – tutto il proprio potenziale[11], è opportuno ampliare e sviluppare un approfondito dibattito scientifico sul tema, non solo al fine di abbattere o ridurre al minimo – attraverso una sempre maggiore consapevolezza e padronanza della materia – i rischi giocoforza emergenti dalla fruizione di tali *tools* informatici, ma soprattutto allo scopo di rendere costantemente compatibili questi ultimi coi valori del giusto processo, in ossequio ai principi di diritto sanciti dalla carta costituzionale e dalle vincolanti fonti sovranazionali[12].

Ebbene, in tale quadro, si colloca l'analisi dei sistemi di riconoscimento facciale, valutando le opportunità che i medesimi possono offrire[13]

«si pensi a perquisizioni e sequestri su documenti informatici, all'apprensione processuale di e-mail o sms, fino alle captazioni effettuate direttamente tramite virus informatici installati sui *devices* dell'intercettato» (C. Cesari, *Editoriale: L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Revista Brasileira de Direito Processual Penal*, Porto Alegre, 2019, vol. 4, num. 3, p. 1169, Instituto Brasileiro de Direito Processual Penal).

[11] Molto interessante, sul punto, è il contributo di C. Parodi, V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *Diritto penale contemporaneo*, Milano, 2019, fasc. 6, p. 47, Associazione "Progetto giustizia penale", all'interno del quale gli Autori evidenziano come si imponga «l'esigenza di chiarire entro quali limiti (…) [le] forme di utilizzo di intelligenza artificiale possano entrare nel patrimonio investigativo, cognitivo e valutativo del sistema penale», nell'ottica di «coniugare le enormi potenzialità del settore con le esigenze di efficienza, di prevenzione e repressione di varie forme criminali, assicurando allo stesso tempo piena tutela alle garanzie dei singoli consociati». Vale anche la pena considerare, sul punto, la prospettiva offerta da, D. Polidoro, *Tecnologie informatiche e procedimento penale: la giustizia penale "messa alla prova" dall'intelligenza artificiale*, in *Archivio penale web*, Pisa, 2020, fasc. 3, p. 2, Pisa University Press, consultato – da ultimo – in data 06 dicembre 2024 alla pagina *web* https://archiviopenale.it/File/DownloadArticolo?codice=8f90d1bc-acef-4725-8fd3-c256a7934831&idarticolo=25993, secondo cui l'intelligenza artificiale non ha ancora espresso – in termini di incidenza sul processo penale – tutto il proprio potenziale anche «a causa dello scarso impiego che, sino ad ora, ha avuto all'interno degli ordinamenti giuridici continentali, al contrario, invece, di quanto avvenuto oltre oceano, laddove i giudici utilizzano, ormai da tempo, gli algoritmi "intelligenti" per risolvere alcune problematiche di propria competenza».

[12] D. Polidoro, *op. cit.*, p. 2.

[13] Sul punto, vale la pena richiamare le riflessioni spiccatamente interessanti percorse da J. Della Torre, *Algoritmi di facial recognition e procedimento penale italiano*, in I. Micheli (a cura di), *Ragioni Comuni 2019 - 2020. Risultati delle attività progettuali realizzate tramite assegni di ricerca finanziati dalla Regione Friuli Venezia Giulia ai sensi della LR 34/2015, art. 5, c. 29-33*, Trieste, 2023, p. 172, EUT Edizioni Università di Trieste. Come evidenziato dall'Autore, i sistemi di riconoscimento facciale possono essere impiegati «tanto per finalità di stretta identificazione (cioè per verificare la corrispondenza tra iden-

e, al contempo, esaminando le criticità che possono emergere dal loro utilizzo, anche alla luce della recente introduzione, nel panorama delle fonti giuridiche europee, dell'*Artificial Intelligence Act*.

2. *Una breve ricognizione sui sistemi di riconoscimento facciale*

Allorquando ci si riferisce ai sistemi di riconoscimento facciale, ci si muove nel campo di quella tecnologia dell'identificazione biometrica concernente la possibilità di avvalersi di dispositivi *hardware*[14] e componenti *software*[15], allo scopo di verificare l'identità di una persona mediante l'individuazione di un suo particolare connotato fisico: il volto[16]. Sgomberando il campo da ogni possibile equivoco, è d'uopo precisare come l'attività di riconoscimento di un volto, da parte delle forze di polizia, si riferisce ad un procedimento investigativo che – anche in passato – veniva utilizzato al fine di appurare l'identità di un soggetto sconosciuto. Oggigiorno, tuttavia, questa nuova modalità di "trattamento" dell'immagine facciale, caratterizzata dall'impiego di recentissime tecnologie al fine di addivenire ad un riconoscimento di un viso non conosciuto, rappresenta un'innovazione che, se da un lato entusiasma per la sua dirompente effi-

tità fisica e identità anagrafica di una persona), quanto per riscostruire l'attività criminosa. Il fatto che un *software* riconosca il volto di una persona su una scena del crimine può, del resto, rappresentare un'informazione preziosa, sia per orientare le indagini, sia in chiave probatoria».

[14] Come evidenziato in G. Felluga, *I computer crimes definizioni ed elementi principali*, in *Tigor; Rivista di scienze della comunicazione e di argomentazione giuridica*, Trieste, 2012, fasc. 1, p. 33, EUT Edizioni Università di Trieste, «per hardware si intende l'unità centrale, le memorie e le periferiche; ovvero tutte le parti fisiche di un personal computer (magnetiche, ottiche, meccaniche ed elettroniche) che ne consentono il funzionamento».

[15] Senza volerci qui addentrare nel complesso gorgo nozionistico sedimentatosi sull'argomento, è possibile, tuttavia, precisare come «per *software* si intende l'insieme dei programmi di elaborazione che permettono a un computer di operare» (G. Felluga, *op. cit.*, p. 33).

[16] Sul punto, taluni usano l'acronimo "TRF" per denominare le tecnologie di riconoscimento facciale (anche note come *face detection systems*), ossia «i sistemi in grado di identificare o autenticare una persona a partire dalle caratteristiche del volto» (vedasi, *ex multis*, M. Colacurci, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale*, Milano, 12 Settembre 2022, p. 2, Associazione "Progetto Giustizia Penale", consultato – da ultimo – in data 08 dicembre 2024 alla pagina *web* https://www.sistemapenale.it/pdf_contenuti/1662670043_colacurci-riconoscimento-facciale.pdf).

cienza e potenzialità d'uso, dall'altro lato spaventa per i numerosi interrogativi che instilla tra gli studiosi interessati alla materia.

Nello specifico, i sistemi di riconoscimento facciale si basano su metodi (automatici o semi-automatici) «che registrano e paragonano 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»[17]. La peculiarità di questi metodi di riconoscimento facciale sta dunque nel fatto che essi sono "artificiali", nel senso che l'operazione di identificazione e/o individuazione del viso avviene – interamente o parzialmente – per il tramite di "macchine", oltrepassando quindi la tradizionale attività di "accertamento" compiuta dagli esseri umani (i quali, solitamente, si riconoscono tra loro mediante una ricognizione *de visu*).

Ergo, tale operazione di riconoscimento muove, in primo luogo, dall'acquisizione – da parte di uno o più dispositivi *hardware* – di un dato biometrico «rappresentato dall'immagine di un volto umano»[18], che avviene tramite sensori deputati alla registrazione di un'immagine (oppure di una serie di immagini) del viso di un certo soggetto e delle sue caratteristiche più rilevanti[19] (si pensi, ad esempio, alla forma dalla faccia, alla distanza tra gli occhi, alla conformazione del naso, all'ampiezza della fronte, ecc.)[20]. Compiuta l'estrazione del dato biometrico, le immagini così "prelevate" vengono "elaborate" da un algoritmo deputato a riscontrare, al loro interno, le principali caratteristiche facciali (c.d. *features*) dell'effige analizzata, onde poi convertirle – in guisa di una «rappresentazione numerica che distingue univocamente una persona»[21] – in formato

[17] Si rimanda, sul punto, all'accuratissimo contributo in materia redatto da E. Sacchetto, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, in *Diritto penale contemporaneo*, Milano, 2019, fasc. 2, p. 470, Associazione "Progetto giustizia penale".

[18] Vedasi, sul punto, J. Della Torre, *Algoritmi di facial recognition e procedimento penale italiano*, *op. cit.*, p. 169.

[19] Anche in questo caso risulta preziosissimo il contributo di E. Sacchetto, *Spunti per una riflessione sul rapporto fra biometria e processo penale*, *op. cit.*, p. 470.

[20] Vale la pena sottolineare come l'acquisizione – da parte di uno o più dispositivi *hardware* – della figura di un volto umano può avvenire, oltre che mediante l'utilizzo di sensori deputati alla registrazione di un'immagine (oppure di una serie di immagini) del viso di un certo soggetto, anche attraverso l'estrazione del dato biometrico di una faccia ritratta in una fotografia (*cfr.* M. Colacurci, *op. cit.*, p. 2).

[21] G. Mobilio, *L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?*, in *La democrazia della società digitale; tensioni e opportunità*, in E. Di Carpegna Brivio e al. (a cura di), Torino, 2023, p. 4, Giappichelli Editore.

digitale e realizzare, dunque, un *template*, ossia un modello la cui funzione è quella di essere utilizzato per riscontrare una sua eventuale corrispondenza con altre immagini (riferite alla persona che si vuole identificare) contenute in banche dati precedentemente allestite[22]. All'esito di questa procedura di comparazione, qualora emerga un'effettiva congruenza tra i predetti termini di paragone (il *template* artificialmente modellato del viso di una persona ed un'immagine già archiviata della medesima), l'operazione di riconoscimento darà un esito positivo, in guisa di un'avvenuta identificazione dell'individuo di cui si voleva appurare (e/o confermare) l'identità. Occorre, comunque, precisare come l'anzidetta corrispondenza tra persone già "schedate" e il volto della cui identità ci si interroga riguarda un processo probabilistico in cui il *software* di riconoscimento facciale esprime la somiglianza delle immagini comparate «tramite un valore percentuale chiamato "*similarity score*": più alto è questo punteggio, più alta sarà la probabilità che l'immagine campione raccolta corrisponda a quella nella galleria» o banca dati preallestita[23]. A fronte di tale operazione di "raffronto", spetterà poi all'operatore umano confermare o disattendere il risultato fornito – in termini probabilistici – dalla "macchina".

Così delineato, in linea generale, il meccanismo di funzionamento dei sistemi di riconoscimento facciale, non sfuggirà, quindi, come siffatti strumenti – le cui potenzialità sono già intrinsecamente sorprendenti[24] –

[22] Cfr. G. Mobilio, *Tecnologie di riconoscimento facciale; rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021, p. 11, Editoriale Scientifica.

[23] G. Mobilio, *L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?*, *op. cit.*, p. 4-5.

[24] Con riferimento al grande potenziale degli strumenti di riconoscimento facciale è utile tenere in considerazione anche A. Pin, *Non esiste la "pallottola d'argento": l'Artificial Face Recognition al vaglio giudiziario per la prima volta*, in *Diritto pubblico comparato ed europeo (DPCE) online*, Milano, 2019, fasc. 4, p. 3076, Università commerciale "L. Bocconi", consultato – da ultimo – in data 06 dicembre 2024 alla pagina *web* https://www.dpceonline.it/index.php/dpceonline/article/view/873/851, il quale propone un'attenta disamina della sentenza "R (Bridges) v. The Chief Constable of South Wales Police et al." emessa dalla High Court of Justice dell'Inghilterra e Galles, che merita di essere approfondita poiché rappresenta uno dei primissimi approdi giurisprudenziali – se non addirittura il primo – in materia di «utilizzo dell'Artificial Face Recognition (AFR) nella previsione e nella individuazione dei reati». All'interno di questa sentenza si ammette come il riconoscimento facciale si manifesti innegabilmente quale «tecnologia dal grande potenziale per "la prevenzione e l'individuazione del crimine, la cattura dei sospetti o dei colpevoli e la protezione del pubblico", di gran lunga superiore alle tecniche che semplicemente riprendono i passanti». Come evidenziato dall'Autore, tuttavia nel medesimo

divengano ancor più efficaci, ed esponenzialmente "potenti", allorquando siano affiancati all'intelligenza artificiale, ossia quando i *face detection systems* siano designati per funzionare attraverso algoritmi[25] in grado non soltanto di apprendere autonomamente tutte le informazioni necessarie all'identificazione di una persona, ma anche di svolgere – senza l'intervento di alcun apporto umano (o riducendo quest'ultimo ad un contributo "marginale") – le operazioni di riconoscimento di tale individuo. In tal caso, è dunque possibile riferirsi al concetto di *automated facial recognition systems* (cosiddetti "AFRS"), ossia di strumenti di riconoscimento facciale che consentono «di analizzare in diretta i flussi video *live* provenienti dalle telecamere presenti in una zona; di selezionare dai *frame* delle immagini le impronte facciali delle persone riprese e di cercare, infine,

provvedimento giudiziale la Corte *de qua* rileva come il ricorso a tali strumenti faccia emergere anche «aspetti inquietanti», posto che i *tools* di riconoscimento facciale possono autonomamente elaborare «i dati biometrici della popolazione su larga scala e senza il coinvolgimento di quest'ultima». In merito a questa pronuncia della High Court of Justice dell'Inghilterra e Galles ha scritto anche J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, in *Diritto penale contemporaneo*, Milano, 2020, fasc. 1, p. 234, Associazione "Progetto giustizia penale", consultato – da ultimo – in data 11 dicembre 2024 alla pagina *web* https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_1_2020_Della%20torre.pdf, il quale evidenzia l'importanza di tale sentenza poiché, seppur giunta a conclusioni interpretative non pienamente condivisibili (tant'è che, come sottolineato acutamente dall'Autore, questa decisione – «lungi dall'essere riuscita a dirimere il contrasto tra sostenitori e oppositori del riconoscimento facciale – è andata incontro ad accese critiche, sollevate da una pluralità di soggetti»), si manifesta tuttavia come «il primo arresto a livello mondiale ad aver affrontato in modo analitico la questione della compatibilità dell'utilizzo da parte della polizia di mezzi di riconoscimento facciale con i diritti fondamentali alla riservatezza e alla tutela dei dati personali» (*ivi*, p. 239).

[25] Un'interessante "prospettiva storica" di algoritmo la si può rinvenire nella sentenza n°7003 pronunciata – il 14 novembre 2022 – dalla terza sezione del T.A.R. Campania e oggetto della nota di E. Falletti, *Mai accettare caramelle né atti amministrativi da sconosciuti, ancorché algoritmi*, in *Il diritto dell'informazione e dell'informatica*, Giuffrè Francis Lefebvre, Milano, 2023, fasc. 1, pagg. 93-94: «l'algoritmo, sin dalla nozione desunta dai papiri di Ahmes del XVII secolo a.c., consiste in una sequenza finita e ordinata di operazioni elementari e chiare di calcolo che permettono di risolvere, in maniera determinata, un problema. Si tratta di una procedura di calcolo ben definita che consente, attraverso un insieme di operazioni effettuate in un determinato ordine, partendo da un insieme di dati (input), di ottenere un risultato atteso (output)». La stessa Autrice, nella propria nota, offre altresì uno spunto bibliografico proprio in tema di nozione di algoritmo, richiamando peraltro l'attenzione sulla pivotale opera di A. M. Turing, *Computer machinery and intelligence*, in *Mind*, New Series, 1950, Vol. 59, fasc. 236, p. 433-460, Oxford University Press.

un *match* tra quest'ultime e i volti contenuti in un archivio di partenza»[26]. Tale modalità operativa di questi strumenti viene sovente definita *real-time*, cioè "in tempo reale", onde richiamare l'attenzione sull'aspetto più caratteristico in seno alla procedura di riconoscimento facciale, ossia la capacità dei medesimi «non solo di identificare in modo più rapido persone di cui non si conosca l'identità, ma anche di conoscere in tempo reale se un certo individuo, sospettato di aver compiuto (o di poter commettere) un reato, possa trovarsi in un determinato luogo, sottoposto a osservazione»[27].

Oltre a questa funzione di riconoscimento facciale, tali strumenti – sfruttando le potenzialità offerte dall'intelligenza artificiale – sono quindi in grado non soltanto di acquisire caratteristiche biometriche e i tratti somatici di un volto ai fini dell'identificazione di una certa persona, bensì possono anche accertare comportamenti che si ipotizza siano sospetti – come accade, ad esempio, nei casi di vagabondaggio (cosiddetta funzione di *loitering detection*) – ovvero individuare assembramenti pericolosi o, ancora, rilevare movimenti "insoliti" delle masse e, finanche, riconoscere lo stato emotivo dei soggetti "monitorati"[28]. Codesta funzione di sorveglianza da parte delle autorità di polizia potrebbe anche dispiegarsi, eventualmente, non soltanto allo scopo di individuare un soggetto, ma anche di tipizzare una certa persona in determinate categorie, mediante l'estrazione di «alcune caratteristiche dall'immagine facciale, come l'età, le origini etniche, il genere, lo stato di salute»[29].

Questa modalità di riconoscimento facciale "in tempo reale" che, a primo impatto, potrebbe sembrare soltanto una mera ipotesi fantascientifica è, invece, una concreta ed attuale possibilità tecnologica di cui molti soggetti giuridici – privati ed istituzionali – possono oggigiorno avvalersi. In Italia, ad esempio, l'azienda leccese "Parsec 3.26" ha elaborato

[26] J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della High Court of Justice*, *op. cit.*, p. 233.

[27] *Ivi*, p. 232.

[28] *Cfr.* W. Nocerino, *Sulle modalità di acquisizione delle immagini provenienti dalle telecamere di videosorveglianza*, in *Cassazione penale*, Milano, 2024, fasc. 7-8, p. 2423, Giuffrè Francis Lefebvre, la quale evidenzia come – a seguito dei sorprendenti sviluppi dell'intelligenza artificiale e dell'esponenziale miglioramento dei *software* all'uopo dedicati – il fenomeno del monitoraggio degli individui e del controllo capillare continuativo remoto dei consociati che abitano le moderne "*smart city*" abbia disvelato scenari (finanche di natura giuridica) del tutto inimmaginabili, persino nel più recente passato.

[29] G. Mobilio, *L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?*, *op. cit.*, p. 5.

un *software* di riconoscimento facciale denominato "SARI" (ossia, "sistema automatico di riconoscimento immagini") che può funzionare anche in modalità *real time*. Più specificamente, quest'azienda – su incarico del Ministero dell'Interno[30] – ha elaborato un *software*, in grado di analizzare immagini e video, che permette il riconoscimento automatico dei volti in due scenari operativi, definiti dalla stessa Autorità ministeriale *enterprise* e *real-time*. La ragione dello sviluppo di un siffatto *software* sta nella volontà, espressa dallo stesso Ministero dell'Interno, di affiancare questo nuovo strumento di riconoscimento facciale al «sistema AFIS-SSA, per fornire all'operatore un efficiente supporto informatico che ne agevoli l'attività di indagine»[31].

La modalità definita *enterprise* del suddetto *software* è stata ideata per rispondere all'esigenza di acclarare l'identità di un volto presente in un'immagine mediante una ricerca[32] – compiuta in automatico, per mezzo di uno o più algoritmi di riconoscimento facciale – all'interno di una banca dati di grandi dimensioni (dell'ordine di milioni di immagini circa) contenente le generalità e le caratteristiche (anche biometriche) di persone già fotosegnalate o schedate. Conclusasi questa attività automatica di elaborazione dati, il *software* (declinato nello scenario *enterprise*) offre all'operatore una lista di volti simili a quello ricercato la quale viene ordi-

[30] Vedasi approfonditamente, su questo punto, Ministero Dell'interno (Dipartimento Della Pubblica Sicurezza), *Capitolato tecnico: procedura volta alla fornitura della soluzione integrata per il sistema automatico di riconoscimento immagini S.A.R.I. (Lotto N° 1)*, consultato – da ultimo – in data 11 dicembre 2024 alla pagina *web* https://www.poliziadistato.it/statics/06/20160627-ct-sari--4-.pdf, p. 6.

[31] Garante Per La Protezione Dei Dati Personali, *Sistema automatico di ricerca dell'identità di un volto*, provvedimento n°440 del 26 luglio 2018, doc. *web* n°9040256, consultato – da ultimo – in data 06 dicembre 2024 alla pagina *web* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9040256. Come esplicato in R. Biondo, *La banca dati nazionale dna italiana*, in *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)*, Milano, 2016, fasc. 1, p. 216, Giuffrè Francis Lefebvre, l'acronimo "AFIS" sta ad indicare l'espressione inglese *automated fingerprint identification system* e si riferisce al sistema che acquisisce e gestisce le impronte digitali in uso al «Casellario centrale d'identità del Ministero dell'interno, Dipartimento della pubblica sicurezza collocato presso la Direzione centrale anticrimine della Polizia di Stato, Servizio polizia scientifica».

[32] In base a quanto stabilito nel predetto capitolato tecnico ministeriale, l'operatore può limitare la ricerca dell'identità di un volto ad una singola banca dati o ad una porzione di essa, filtrandola sulla base di informazioni anagrafiche o descrittive (sesso, altezza, ecc.) associate alle immagini; peraltro, nel caso in cui all'interno dell'immagine da analizzare siano presenti più volti, il *software* consente all'operatore anche la possibilità di selezionare il (singolo) viso da ricercare (*ivi*, p. 6).

nata in base ad un "punteggio" che ne indichi il grado di similarità; a questo punto, l'operatore "umano" ha il compito di «confermare o meno il risultato del *tool*, applicando le procedure di comparazione fisionomica, rispetto alle quali le forze di polizia scientifica ricevono una specifica formazione»[33].

Quanto allo «scenario *real-time*» del *software* elaborato dalla "Parsec 3.26", si tratta invece di una soluzione di riconoscimento automatico dei volti operante «in un'area geografica ristretta e ben delineata» e basata sulla necessità di «analizzare in tempo reale i volti dei soggetti ripresi dalle telecamere ivi installate confrontandoli con una banca dati ristretta e predefinita (denominata "watch-list") la cui grandezza è dell'ordine delle centinaia di migliaia di soggetti»[34]. La peculiarità di questo «scenario *real-time*» concerne quindi la possibilità di visionare «in tempo reale più volti presenti contemporaneamente nei fotogrammi dei video in ingresso», all'uopo «ottenuti dalle telecamere installate in molteplici punti di osservazione a supporto di operazioni di controllo del territorio in occasione di eventi e/o manifestazioni»: riscontrata un'eventuale corrispondenza tra il fotogramma del video ed un volto presente nella "watch-list", il *software* genererà «un alert in grado di richiamare l'attenzione degli operatori»[35].

Tra i due scenari operativi sussiste dunque una differenza assolutamente non trascurabile. Nel sistema SARI *enterprise* la funzione è quella di cercare l'identità di un volto a partire da immagini statiche contenute su banche dati di enormi dimensioni («dell'ordine di 10 milioni di immagini»), allo scopo di addivenire ad una lista di risultati "simili" a quello ricercato da sottoporre poi all'attenzione di un operatore (il quale dovrà, materialmente, procedere all'identificazione); nel sistema SARI *real-time*, invece, si procede con un riconoscimento in tempo reale di volti presenti in flussi video provenienti da telecamere, mediante un algoritmo che – in maniera completamente autonoma – confronterà i volti presenti nei flussi video con quelli di una *watch-list* (avente una grandezza dell'ordine di 100.000 identità preinserite in banca dati), onde fornire un *alert* in caso di positiva corrispondenza tra il fotogramma acquisito ed il volto ricercato, senza necessità di alcun intervento umano nella procedura di identificazione[36].

[33] J. Della Torre, *Algoritmi di facial recognition e procedimento penale italiano*, *op. cit.*, p. 171.

[34] Ministero Dell'interno (Dipartimento Della Pubblica Sicurezza), *op. cit.*, p. 6.

[35] *Ibidem*.

[36] *Ibidem*.

Punto in comune, per converso, dei due scenari operativi anzidetti è la intrinseca necessità che, al termine delle operazioni analitico-computazionali eseguite dal *software* (tanto nella sua declinazione *enterprise* quanto nella versione *real-time*), vi sia sempre un intervento umano "finale" cui spetta il compito di confermare il riconoscimento ipotizzato dall'algoritmo «e di prendere i provvedimenti conseguenti»[37].

Questa "divergenza" operativa tra le predette modalità di funzionamento del sistema SARI si riflette non soltanto nel concreto impiego del *software* da parte delle autorità istituzionali, ma si riverbera inevitabilmente anche sui profili di legittimità ed ammissibilità di codesto strumento, come sarà specificato nel paragrafo successivo.

3. *Le criticità dei sistemi di riconoscimento facciale con riguardo al processo penale; problemi di una disciplina normativa ancora "incompiuta"*

. Ancorché foriero di innegabili vantaggi, l'utilizzo dei sistemi di riconoscimento facciale pone – come già accennato – numerosi interrogativi circa la sua compatibilità con le garanzie costituzionali e coi principi del giusto processo penale. Tali sistemi, infatti, comportano necessariamente una captazione di un dato biometrico e, per l'effetto, incidono giocoforza sul tema, ad esempio, delle libertà fondamentali e del trattamento dei dati personali[38]. Basti considerare come gli strumenti di cui trattasi siano molto più invasivi «di altre tecnologie biometriche: rispetto alle impronte digitali o ai campioni di DNA, infatti, è molto più facile catturare l'immagine di un volto, dal momento che ciò può avvenire a distanza, con persone in movimento, senza alcun contatto fisico e senza che vi sia alcuna consapevolezza o consenso»[39].

Peraltro, l'utilizzo di tecnologie di riconoscimento facciale comporta

[37] J. Della Torre, *Algoritmi di facial recognition e procedimento penale italiano*, *op. cit.*, p. 171.

[38] Più in generale (come rilevato da G. Mobilio, *L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?*, *op. cit.*, p. 2-3), l'interrogativo scaturente dall'utilizzo delle tecnologie di riconoscimento facciale concerne la compatibilità delle medesime non solo alla disciplina sulla protezione dei dati personali, ma anche – e soprattutto – ai diritti fondamentali tutelati dagli ordinamenti democratici, allo scopo di stabilire quali siano le condizioni ed i limiti per l'uso di siffatti strumenti in modo da indirizzarne l'impiego verso valori costituzionali.

[39] G. Mobilio, *L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?*, *op. cit.*, p. 2.

nuovi paradigmi anche in tema di diritto processuale penale (unico ambito giuridico che sarà qui trattato) poiché crea scenari inediti sia all'interno della fase delle indagini preliminari, sia nell'arco dell'intera vicenda dibattimentale. Senza ripercorrere le considerazioni già intraprese *supra*, si vuole tuttavia rimarcare come il "rito" penale si trovi, attualmente, a confrontarsi con tecnologie inedite il cui impiego potrebbe arrecare – a ben vedere – rischi maggiori (in termini di "tenuta" normativa) rispetto agli auspicati benefici.

Il punto di partenza nell'affrontare il dibattito emergente (in seno alla scienza processual-penalistica) circa l'impiego di tali sistemi di riconoscimento non può non scaturire dalla presa di coscienza per cui l'accesso ad immagini facciali (o, più in generale, a qualunque dato biometrico) deve essere considerato come un'ingerenza nella vita delle persone e può trovare giustificazione soltanto allorquando esso trovi fondamento in una specifica base normativa[40]. Tuttavia, il punto chiave della questione sta proprio nel fatto che ad oggi, all'interno dell'ordinamento italiano, non esiste alcuna specifica disposizione che legittimi espressamente – con riguardo al processo penale – l'impiego dei sistemi di riconoscimento facciale. In ragione di tale lacuna normativa, si è cercato di validare l'impiego di tali nuove tecnologie mediante il richiamo a disposizioni già esistenti, muovendo però dalla consapevolezza che, *ab origine*, il riconoscimento facciale si configura come una modalità di trattamento di dati biometrici ed afferisce, anzitutto, alla materia della tutela e della protezione dei dati personali, entrambe intese quali corollari di quella libertà fondamentale dell'individuo sancita all'art. 8 della Carta dei diritti fondamentali dell'Unione europea[41].

Poiché, ai sensi dell'art. 8 testé citato[42], il rispetto delle regole sulla protezione dei dati di carattere personale deve essere soggetto al controllo di un'autorità indipendente, in relazione all'ordinamento italiano diviene dunque fondamentale considerare, in primo luogo, la posizione assunta dal Garante per la protezione dei dati personali.

Da questo punto di vista, il Garante per la protezione dei dati persona-

[40] Cfr. S. El Sabi, *La violazione della privacy in caso di raccolta "sistematica" dei dati biometrici e genetici: lesi i diritti e le libertà della persona interessata?*, in *Giustizia civile.com*, Milano, 2023, vol. 10, fasc. 5, p. 9-10, Giuffrè Francis Lefebvre.

[41] Infatti, l'art. 8 della Carta dei diritti fondamentali dell'Unione europea (rubricato «protezione dei dati di carattere personale») stabilisce, al suo primo comma, che «ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano».

[42] Vedasi il comma 3 dell'art. 8 della Carta dei diritti fondamentali dell'Unione europea.

li ha emesso un proprio parere circa le eventuali criticità insorgenti dall'utilizzo – sotto il profilo del trattamento di dati personali nonché della loro pedissequa protezione – «di un sistema automatico di ricerca dell'identità di un volto presente in un'immagine facciale all'interno di una banca dati, denominato "SARI Enterprise"»[43]. Ciò che qui rileva, è che secondo tale Autorità, «il trattamento dei dati biometrici ricavabili anche dall'immagine facciale, effettuato dalle forze di polizia a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, è previsto e disciplinato da una pluralità di fonti normative (quali l'art. 4 del T.U.L.P.S., approvato con regio decreto 18 giugno 1931, n. 773 e art. 7 del relativo regolamento di esecuzione, approvato con regio decreto 6 maggio 1940, n. 635; l'art. 349 del codice di procedura penale; l'art. 11 del decreto legge 21 marzo 1978, n. 59, convertito in legge 18 maggio 1978, n. 191; l'art. 5 del decreto legislativo 25 luglio 1998, n. 286)»[44]. Codesta Autorità, inoltre, richiama anche le fonti di diritto europeo e si sofferma, in particolare, sul Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (ossia, sul Regolamento generale sulla protezione dei dati), per quanto concerne il trattamento dei dati biometrici (ivi compresi quelli ricavabili dall'immagine facciale)[45].

In particolare, il Garante, dovendosi esprimere sulla modalità operativa del SARI *enterprise*, ha ritenuto che eventuali criticità di tale sistema non sono riscontrabili in tale "scenario", posto che quest'ultima declinazione del *software* in esame compie un trattamento dei dati personali estrinsecantesi in un «mero ausilio all'agire umano, avente lo scopo di velocizzare l'identificazione, da parte dell'operatore di polizia, di un soggetto ricercato della cui immagine facciale si disponga, ferma restando l'esigenza dell'intervento dell'operatore per verificare l'attendibilità dei risultati prodotti dal sistema automatizzato»[46]. Infatti, seguendo le argomentazioni del Garante, il SARI *enterprise* si configurerebbe come un

[43] Garante Per La Protezione Dei Dati Personali, *Sistema automatico di ricerca dell'identità di un volto*, *op. cit.*

[44] *Ibidem*.

[45] Questa sede non consente di approfondire, per esigenze di sinteticità, l'interessante *iter* giuridico intrapreso dal Garante Per La Protezione Dei Dati Personali all'interno del provvedimento n. 440 del 26 luglio 2018, che merita attenzione poiché non soltanto ripercorre analiticamente le normative europee di riferimento, ma anche perché riassume – in maniera esauriente – i tratti salienti del funzionamento del sistema SARI e dei suoi scenari operativi *enterprise* e *real-time*.

[46] Garante Per La Protezione Dei Dati Personali, *Sistema automatico di ricerca dell'identità di un volto*, *op. cit.*

upgrade dell'AFIS: quest'ultimo già «consente di effettuare ricerche nell'archivio dei soggetti fotosegnalati (…) tramite l'opera manuale di un operatore, che deve inserire nei campi presenti nella maschera di interrogazione informazioni anagrafiche, connotati e contrassegni (ad esempio, colore dei capelli, degli occhi, di tatuaggi), al fine di individuare la presenza nell'archivio AFIS del soggetto ricercato»[47]. Il SARI *enterprise*, dal canto suo, non serve a compiere elaborazioni aggiuntive rispetto al sistema AFIS, ma automatizza, invece, «alcune operazioni che prima richiedevano l'inserimento manuale di connotati identificativi, consentendo le operazioni di ricerca nel data base dei soggetti fotosegnalati attraverso l'inserimento di una immagine fotografica, che sarà elaborata automaticamente al fine di fornire l'elenco di foto segnaletiche somiglianti, ottenute attraverso un algoritmo decisionale che ne specifica la priorità»[48].

Il Garante per la protezione dei dati personali si è espresso, in seguito, anche in tema di SARI *real-time*, evidenziando come questa modalità di riconoscimento (orientata «all'effettuazione di un trattamento di dati personali per finalità di prevenzione di reati e minacce alla sicurezza pubblica e, anche su delega dell'Autorità Giudiziaria, di indagine, accertamento e perseguimento di reati»), poiché determina «una forte interferenza con la vita privata delle persone interessate», deve trovare giustificazione in una adeguata base normativa che, attualmente, non è tuttavia rinvenibile all'interno di alcuna specifica disposizione di Legge che consenta tale tipo di trattamento[49]. Peraltro, il Garante non ha ritenuto applicabili quelle fonti normative che il Ministero dell'Interno aveva invece

[47] *Ibidem*.

[48] *Ibidem*.

[49] Garante Per La Protezione Dei Dati Personali, *Parere sul sistema Sari Real Time - 25 marzo 2021*, provvedimento n°127 del 25 marzo 2021, doc. *web* n°9575877, consultato – da ultimo – in data 06 dicembre 2024 alla pagina *web* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877. Interessante è il percorso motivazionale affrontato dal Garante, secondo cui il SARI *real-time* realizza un trattamento di dati biometrici «automatizzato su larga scala che può riguardare, tra l'altro, anche coloro che siano presenti a manifestazioni politiche e sociali, che non sono oggetto di "attenzione" da parte delle forze di Polizia; ancorché la valutazione di impatto indica che i dati di questi ultimi sarebbero immediatamente cancellati, nondimeno, l'identificazione di una persona in un luogo pubblico comporta il trattamento biometrico di tutte le persone che circolano nello spazio pubblico monitorato, al fine di generare i modelli di tutti per confrontarli con quelli delle persone incluse nella "watch-list". Pertanto, si determina una evoluzione della natura stessa dell'attività di sorveglianza, passando dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza universale allo scopo di identificare alcuni individui».

ritenuto conferenti al fine dell'inquadramento e del fondamento giuridico del SARI *real-time*. Nello specifico, l'Autorità Garante non ha ritenuto che gli «articoli del codice di procedura penale (agli artt. 134 c. 4, 234, 266, 431 c. 1 lett. b, oltre gli artt. 55, 348, 354 e 370 sull'attività di polizia giudiziaria)» richiamati dal suddetto Dicastero potessero legittimare l'impiego del sistema SARI *real-time*, giacché codeste disposizioni «non costituiscono base giuridica idonea per trattamenti di dati biometrici diretti all'identificazione personale», in quanto non assurgono a «quella fonte normativa specifica richiesta dall'art. 7»[50] del decreto legislativo 18 maggio 2018, n. 51[51]. In sintesi, la raccolta di dati biometrici (tra cui anche quelli concernenti le immagini facciali), seppur finalizzata e/o funzionale all'identificazione di determinati soggetti, può essere effettuata «solo in presenza di un'idonea previsione normativa ai sensi dell'art. 7 d.lgs. n. 51/2018, che al momento non pare rinvenibile»[52].

Ebbene, la prospettiva offerta dall'Autorità Garante per la protezione dei dati personali agevola nel comprendere come la volontà di una parte della pubblica amministrazione (e finanche della politica)[53] di far entrare in funzione quanto prima, all'interno dell'ordinamento italiano, i sistemi di riconoscimento facciale – onde perseguire i suindicati scopi di investigazione, vigilanza e, più in generale, di contrasto al crimine – sospinga i sostenitori di tali tecnologie a richiamare l'attenzione su certe disposizioni di matrice processual-penalistica, ancorché non specificamente dedicate all'enucleazione di regole in tema di trattamento del dato biometrico facciale, pur di individuarne un fondamento giuridico che ne legittimi l'impiego. Tuttavia, questa prassi contrasta con quanto stabilito

[50] Cfr. Garante Per La Protezione Dei Dati Personali, *Parere sul sistema Sari Real Time - 25 marzo 2021*, *op. cit.*, in cui si richiama il ruolo pivotale dell'art. 7 del decreto legislativo 18 maggio 2018, n. 51, che così dispone: «il trattamento di dati di cui all'articolo 9 del regolamento UE è autorizzato solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento, ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato».

[51] *Ibidem*.

[52] Garante Per La Protezione Dei Dati Personali, *Provvedimento n° 54 del 26 febbraio 2020*, doc. *web* n°9309458, consultato – da ultimo – in data 10 febbraio 2025 alla pagina *web* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9309458.

[53] Cfr. J. Della Torre, *Algoritmi di facial recognition e procedimento penale italiano*, *op. cit.*, p. 176.

espressamente dalle fonti di diritto europeo, a norma delle quali l'utilizzo di tecnologie di riconoscimento facciale per finalità di prevenzione e repressione di reati deve trovare necessariamente giustificazione in una adeguata base normativa, pena la sua inammissibilità[54].

Per tale ragione, in epoca recente il Legislatore italiano è intervenuto con un primo embrione di intervento regolativo circa l'utilizzo dei sistemi di riconoscimento facciale, con lo scopo di consentire l'impiego del SARI e, al contempo, di assicurare il pieno rispetto dei diritti fondamentali sanciti dalle fonti normative europee[55].

Nello specifico, il decreto-legge 8 ottobre 2021, n. 139 (poi convertito, con modificazioni, dalla Legge 3 dicembre 2021, n. 205) all'interno del suo art. 9, comma 9, stabilisce che l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale operanti attraverso l'uso dei dati biometrici in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, sono sospese fino all'entrata in vigore di una disciplina legislativa della materia[56] e comunque non oltre il 31 dicembre 2025[57].

[54] Vale la pena richiamare il dettato dell'art. 9 (rubricato «trattamento di categorie particolari di dati personali») del citato Regolamento (UE) 2016/679, all'interno del quale è enucleato il divieto di trattare «dati biometrici intesi a identificare in modo univoco una persona fisica», salvo i casi particolari enunciati dalla medesima disposizione. In merito al «trattamento di categorie particolari di dati personali» testé accennato interviene anche l'art. 7 del decreto legislativo 18 maggio 2018 n 51 che, in attuazione del predetto art. 9 del Regolamento (UE) 2016/679, stabilisce come esso può essere «autorizzato solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione europea o da legge o, nei casi previsti dalla legge, da regolamento, ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato».

[55] Il richiamo alle fonti europee viene esplicitato dal medesimo Legislatore, il quale – all'*incipit* del predetto art. 9 – chiarisce che, nell'impiego di sistemi di riconoscimento facciale, occorra considerare sia «quanto disposto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016» (ossia, il Regolamento generale sulla protezione dei dati, c.d. "GDPR"), sia «la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016» (cioè, la Direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, c.d. "LED"), nonché il «principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea» allorquando occorra disciplinare l'ammissibilità, le condizioni e le garanzie relativi all'impiego di sistemi di riconoscimento facciale.

[56] Cfr. decreto-legge 8 ottobre 2021, n. 139 (convertito, con modificazioni, dalla Legge 3 dicembre 2021, n. 205) art. 9, comma 9.

[57] Non è da sottovalutare come tale scadenza – fissata dal Legislatore al giorno 31

Al contempo, però, il comma 12 del medesimo art. 9 mitiga la sospensione anzidetta prevedendo che essa non si applica «ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali»[58], allorquando avvengano in presenza di un parere favorevole del Garante per la protezione dei dati personali, «salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero»[59].

Da un'iniziale disamina della suindicata disposizione sembrerebbe come tale dettato normativo enuclei la possibilità – in taluni specifici casi – di adoperare sistemi di riconoscimento facciale, così escludendo l'operatività dei precedenti commi 9, 10 e 11 dell'anzidetto decreto-legge 8 ottobre 2021, n. 139 (per come poi convertito): infatti, lo stesso comma 12 ammette che l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale – operanti attraverso l'uso

dicembre 2025 – sia l'effetto di una "proroga", giacché *ab origine* la citata sospensione dell'installazione e dell'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale (operanti attraverso l'uso dei dati biometrici in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati) rimaneva subordinata non soltanto sino all'entrata in vigore di una disciplina legislativa della materia, ma soprattutto al termine del 31 dicembre 2023. Un siffatto differimento temporale di due anni (quale data di scadenza della sospensione *de qua*) sottolinea, in maniera evidente, come il Legislatore non abbia ancora deciso di regolamentare puntualmente la materia, lasciando dunque che, nell'ordinamento italiano, restino *de facto* inoperanti i sistemi di riconoscimento facciale (specialmente nella loro declinazione "*real-time*").

[58] Il richiamo al decreto legislativo 18 maggio 2018, n. 51 (rubricato «attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio»), si riferisce all'attuazione della già citata direttiva (UE) 2016/680, ossia la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (c.d. "LED"), la quale garantisce la protezione dei dati personali delle persone coinvolte in procedimenti penali, che siano testimoni, vittime o indiziati.

[59] L'art. 9, comma 12, del predetto decreto-legge 8 ottobre 2021, n. 139 (convertito, con modificazioni, dalla Legge 3 dicembre 2021, n. 205) stabilisce, più specificamente, che «i commi 9, 10 e 11 non si applicano ai trattamenti effettuati dalle autorità competenti a fini di prevenzione e repressione dei reati o di esecuzione di sanzioni penali di cui al decreto legislativo 18 maggio 2018, n. 51, in presenza, salvo che si tratti di trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero, di parere favorevole del Garante reso ai sensi dell'articolo 24, comma 1, lettera b), del medesimo decreto legislativo n. 51 del 2018».

dei dati biometrici ed allestiti in luoghi pubblici o aperti al pubblico – possa essere consentita, purché essa sia riconducibile a «trattamenti»[60] effettuati da soggetti all'uopo autorizzati ed espressamente individuati nelle c.d. «autorità competenti»[61] e nella «autorità giudiziaria». È importante sottolineare, tuttavia, come l'autorizzazione all'impiego dei *facial recognition systems* diverga – ai sensi del predetto comma 12 dell'art. 9 – a seconda che la fruizione di tali apparati sia compiuta, da un lato, dalle autorità di pubblica sicurezza o forze di polizia e, dall'altro, dall'autorità giudiziaria. Nella prima ipotesi – ossia nel caso di utilizzo dei sistemi di riconoscimento facciale da parte delle autorità di pubblica sicurezza o delle forze di polizia – il comma 12 dell'art. 9 *de quo* prevede espressamente la necessità di un previo «parere favorevole del Garante reso ai sensi dell'articolo 24, comma 1, lettera b), del medesimo decreto legislativo n. 51 del 2018». Al contrario, se l'impiego dei *facial recognition systems* viene disposto dalla Magistratura (ossia, allorquando ci si riferisce a «trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali nonché di quelle giudiziarie del pubblico ministero»[62]) allora siffatta autorizzazione amministrativa del Garante per la protezione dei dati personali non è in alcun modo richiesta[63].

[60] L'espressione «trattamenti» adoperata dal Legislatore italiano evoca quanto disposto dall'art. 4, comma 1, punto 2, del citato Regolamento generale sulla protezione dei dati, secondo cui – con il termine "trattamento" – ci si riferisce a «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

[61] Il concetto di «autorità competenti», menzionato all'art. 12 del predetto decreto-legge 8 ottobre 2021, n. 139 (convertito, con modificazioni, dalla Legge 3 dicembre 2021, n. 205), deve essere inteso alla stregua della definizione stabilita all'art. 2, comma 1, lett. g, del decreto legislativo 18 maggio 2018, n. 51 (ossia «qualsiasi autorità pubblica dello Stato, di uno Stato membro dell'Unione europea o di uno Stato terzo competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica»). Conseguentemente, in guisa dell'art. 47, comma 1, del medesimo decreto legislativo 18 maggio 2018, n. 51, per «autorità competenti» si fa riferimento alle autorità di pubblica sicurezza o forze di polizia.

[62] Cfr. art. 9, comma 12, decreto-legge 8 ottobre 2021, n. 139 (convertito, con modificazioni, dalla Legge 3 dicembre 2021, n. 205).

[63] Cfr. J. Della Torre, *Algoritmi di facial recognition e procedimento penale italiano*, *op. cit.*, p. 177.

Così ricostruito l'impianto normativo sul quale il Legislatore ha voluto intervenire in merito all'utilizzo dei sistemi di riconoscimento facciale, è d'uopo ciò nonostante evidenziare come lo sfruttamento della tecnologia in esame non possa comunque prescindere dal rispetto delle fonti normative europee e nazionali. Sul punto, occorre difatti considerare come «l'effettiva portata da attribuire al comma 12 dell'art. 9» qui oggetto di esame non vada confusa con un'indiscriminata possibilità – «per determinate istituzioni deputate al contrasto delle attività illecite» – di «utilizzare siffatti strumenti per scopi di prevenzione e di repressione della criminalità in luoghi pubblici e aperti al pubblico», bensì «quale regola volta a ribadire che, anche al netto della moratoria generale nei confronti di tale apparato, le autorità di *law enforcement* possono continuare ad avvalersene, nei *soli casi* e *con i limiti* stabiliti dalle fonti sovraordinate e dal codice di rito»[64].

In sintesi, avuta contezza del generale divieto di utilizzare strumenti di riconoscimento facciale in guisa del comma 9 dell'art. 9 dell'anzidetto decreto-legge 8 ottobre 2021, n. 139 (per come poi convertito), la "deroga" sancita quindi dal pedissequo comma 12 alla fruizione degli AFRS da parte delle forze di polizia e dell'autorità giudiziaria può ritenersi legittima soltanto nell'ipotesi in cui si renda compatibile con tutte quelle vigenti disposizioni di Legge poste a salvaguardia dei diritti della persona, per come tutelati a livello sia europeo che nazionale.

Alla stregua delle considerazioni anzidette, bisogna constatare come nell'intero ordinamento italiano non siano presenti specifiche disposizioni (oltre al summenzionato decreto-legge 8 ottobre 2021, n. 139) che abbiano introdotto nuove discipline *ad hoc* in tema di sistemi di riconoscimento facciale. Ergo, l'unico approccio possibile verso un impiego "processuale" della tecnologia qui in esame consisterebbe nel richiamare dettati normativi afferenti alle norme del rito penale, affinché essi funga-

[64] *Ivi*, p. 177-178. Come osservato da J. Della Torre, una differente esegesi del comma 12 dell'art. 9 *de quo* «finirebbe per esporsi a inevitabili profili di illegittimità costituzionale», dato che tale disposizione non soltanto «non rispetterebbe il rigido vaglio di proporzionalità (in astratto e in concreto), imposto dagli artt. 7,8 e 52 della Carta di Nizza, nonché dall'art. 10 della direttiva 2016/680/UE, quale presupposto essenziale per il legittimo trattamento di dati biometrici, idonei a identificare in modo univoco una persona fisica», ma «non sarebbe neppure idonea a rispettare le condizioni stringenti a cui l'art. 13 Cost. subordina la possibilità di restringere la libertà dell'individuo; difatti, l'art. 9, comma 12, d.l. 139/2021 nulla dice circa i casi e i modi in cui le forze di polizia o la magistratura possono avvalersi dei sistemi di riconoscimento facciale automatico; né specifica alcuna garanzia a salvaguardia dei diritti e le libertà della persona».

no da adeguata base giuridica per conseguire un siffatto obiettivo di fruizione degli AFRS, tenendo sempre a mente la distinzione tra le due modalità operative di tali strumenti.

Avendo riguardo al sistema SARI *enterprise*, il Garante per la protezione dei dati personali, ad esempio, ha concentrato l'attenzione soprattutto sull'art. 349 c.p.p.[65] (ossia sulla disciplina stabilita in tema di identificazione delle persone)[66]: questa disposizione potrebbe, in effetti, fungere da sostrato normativo al fine di rendere possibile «per le forze di polizia e per l'autorità giudiziaria continuare impiegare SARI quale ausilio per le operazioni di identificazione»[67]. In effetti, quando il SARI *enterprise* è impiegato quale ausilio per le operazioni di identificazione *ex* art. 349 c.p.p., non si palesa alcun *vulnus* alle libertà fondamentali dell'individuo sottoposto al riconoscimento facciale, giacché – come ribadito dal Garante stesso – tale sistema si limita semplicemente ad automatizzare alcuni passaggi procedurali insiti nell'*iter* di rilevazione del dato biometrico. Di conseguenza, tale comma 12 dell'art. 9 del decreto-legge 8 ottobre 2021, n. 139 non ha dunque introdotto su questo argomento alcuna riforma palpabile, giacché anche prima dell'entrata in vigore del decreto di cui trattasi (e della sua successiva conversione in legge) era opinione diffusa ritenere che il sistema SARI *enterprise* potesse essere oggetto di legittimazione in guisa del dettato dell'art. 349 c.p.p.

Inversamente, non sono rinvenibili "appigli" processual-penalistici adeguati onde legittimare un'esegesi dell'art. 9, comma 12, del decreto-legge 8 ottobre 2021, n. 139, finalizzata all'impiego del sistema SARI *real-time*, sia perché – come precisato dal Garante per la protezione dei dati personali[68] – non si riscontrano, allo stato attuale, disposizioni codicistiche che soddisfino i requisiti imposti dall'art. 7 del decreto legislativo 18 maggio 2018, n. 51, sia per il fatto che codesta peculiare declinazione del *software* non potrebbe nemmeno assurgere ad una forma (seppur ati-

[65] Qui ci si riferisce, in particolare, alla disciplina dettata dal comma 2 dell'art. 349 c.p.p. (rubricato «identificazione della persona nei cui confronti vengono svolte le indagini e di altre persone»), secondo cui «alla identificazione della persona nei cui confronti vengono svolte le indagini può procedersi anche eseguendo, ove occorra, rilievi dattiloscopici, fotografici e antropometrici nonché altri accertamenti».

[66] Garante Per La Protezione Dei Dati Personali, *Sistema automatico di ricerca dell'identità di un volto*, *op. cit.*

[67] J. Della Torre, *Algoritmi di facial recognition e procedimento penale italiano*, *op. cit.*, p. 178.

[68] Cfr. Garante Per La Protezione Dei Dati Personali, *Parere sul sistema Sari Real Time - 25 marzo 2021*, *op. cit.*

pica) di individuazione o, eventualmente, di ricognizione, pena l'indebita lesione di quelle "guarentigie" che il rito penale pone «a protezione della libertà morale della persona»[69]. Pertanto, anche in quest'ultimo caso tale comma 12 dell'art. 9 del decreto-legge 8 ottobre 2021, n. 139 si palesa come fonte normativa del tutto inadeguata ai fini di una compiuta regolamentazione della materia dei sistemi di riconoscimento facciale di tipo *real-time*, posto che la sua entrata in vigore non è stata accompagnata da alcuna specifica adozione – da parte del Legislatore – di discipline *ad hoc* che legittimassero questa peculiare (e particolarmente invasiva) specie di trattamento dei dati personali.

4. *Conclusioni*

A fronte di questa disamina (giocoforza sintetica, stante l'ampiezza e la significativa complessità del tema affrontato) degli aspetti processual-penalistici connessi e sottesi all'impiego degli strumenti di riconoscimento facciale, viene da chiedersi se, in fin dei conti, l'apporto tecnologico offerto da codesti *tools* giustifichi – in ultima analisi – un sacrificio (più o meno invasivo) delle libertà individuali e, quindi, una loro utilizzazione basata *sic et simpliciter* sulle norme codicistiche vigenti, ovvero se l'introduzione di una siffatta innovazione tecnologica risulti ancora prematura (e, pertanto, differibile) rispetto ad un archetipo di procedimento penale che, nei suoi necessari schematismi, abbisogna di interventi legislativi ponderati e mirati ai fini di una sua rimodulazione finalizzata sia ad accogliere tutte le potenziali novità che sembrerebbero offrire gli AFRS, sia a fronteggiare le eventuali criticità che detti *software* potrebbero far emergere.

Nel tentativo di rispondere a tale interrogativo, occorre preliminarmente constatare come manchi, a tutt'oggi, una seria e concreta volontà di regolamentare esaustivamente l'impiego dei *devices* di riconoscimento facciale, al di là dell'insoddisfacente testo normativo cristallizzatosi nell'art. 9 del decreto-legge 8 ottobre 2021, n. 139. Ciò è desumibile, ad esempio, proprio considerando come la summenzionata sospensione di cui all'art. 9, comma 9, del citato decreto-legge (originariamente fissata al

[69] J. Della Torre, *Algoritmi di facial recognition e procedimento penale italiano*, *op. cit.*, p. 178. *Ivi* l'Autore richiama l'art. 189 c.p.p. quale "barriera" di protezione verso un impiego «insidioso» degli AFRS, i cui "puntelli" possono essere ravvisati pure nel dettato degli artt. 64, comma 2, 188 e 220, comma 2, c.p.p.

31 dicembre 2023), anziché essere sostituita da «una disciplina legislativa della materia», è stata invece prorogata *ex lege* al 31 dicembre 2025[70].

In secondo luogo, nonostante le "spinte" europee ad enucleare una disciplina *ad hoc* sul tema dei sistemi di riconoscimento facciale, il Legislatore nazionale è rimasto ancora pressoché inerte, demandando alle Autorità amministrative l'arduo compito di scandagliare – all'interno dell'ordinamento italiano – un sostrato normativo estendibile anche all'ambito degli AFRS. Tale orientamento attendista, tuttavia, non solo appare disattento verso gli obblighi sovranazionali incombenti nei confronti dello Stato italiano, ma inoltre cozza con i principi (anche costituzionali) in virtù dei quali non è consentito comprimere le libertà personali pur di dare spazio all'applicazione di strumenti tecnologici che non siano ancora giustificati né legittimati – nella loro utilizzazione – da una precisa base giuridica. Questa inadempienza, peraltro, diviene ancor più grave considerando le nuove sfide stimolate dal recentissimo "*Artificial Intelligence Act*" (ossia il c.d. "regolamento sull'intelligenza artificiale")[71]. La portata dirompente di tale regolamento incide, inevitabilmente, anche sul tema degli strumenti di riconoscimento facciale, giacché questi *tools* sovente si avvalgono, nell'espletamento della loro attività, dei meccanismi computazionali operanti attraverso la stessa intelligenza artificiale.

Tra le ragioni di tale inerzia non si può sottacere come la tematica in esame, in guisa della sua spiccata complessità tecnica (derivante dalla compenetrazione di concetti scientifici e giuridici) ingeneri nei confronti dell'interprete non poche difficoltà ricognitive, che sovente si traducono in una scarsa comprensione del modo in cui il "mezzo informatico" operi e come incida, al contempo, nelle dinamiche processuali. Codesta scarsa comprensione potrebbe riverberarsi, conseguentemente, non soltanto in sede di dibattito legislativo, ma anche in seno all'opinione pubblica, così complicando la formazione di una "coscienza" – comune e condivisa – circa i benefici, le implicazioni e gli svantaggi scaturenti dall'applicazione degli AFRS.

Non è nemmeno da sottovalutare, inoltre, come questa inattività del

[70] Cfr. art. 9, comma 9, decreto-legge 8 ottobre 2021, n. 139 (convertito, con modificazioni, dalla Legge 3 dicembre 2021, n. 205).

[71] Ci si riferisce, qui, al «Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale», avente lo scopo di promuovere, in tutta Europa, un utilizzo affidabile di tale strumento. Questo regolamento riveste un'enorme importanza poiché rappresenta il primo quadro giuridico globale, in assoluto, sull'intelligenza artificiale a livello mondiale.

Legislatore potrebbe eventualmente discendere da una volontà (più o meno implicita) di aprire indiscriminatamente «al riconoscimento facciale di massa», sfruttando un'interpretazione particolarmente estensiva delle norme processual-penalistiche, giustificata da intento di prevenzione e di repressione della criminalità in luoghi pubblici e aperti al pubblico[72].

Ebbene, quali che siano, in concreto, le motivazioni alla stregua delle quali ad oggi – all'interno dell'ordinamento italiano – non sia ancora stata introdotta una disciplina specifica in tema di riconoscimento facciale, appare necessario intervenire mediante l'adozione di una normativa che, conformemente ai requisiti imposti dal diritto europeo, consenta a livello nazionale di regolamentare l'impiego di codesti *tools*, legittimandone l'impiego solo allorquando esso non pregiudichi i diritti e le libertà fondamentali della persona.

Si auspica, dunque, che il Legislatore prenda coscienza dell'impellente necessità di dotare l'ordinamento italiano di una disciplina che regoli, in sede procedimentale, l'utilizzo dei sistemi di riconoscimento facciale, affinché il processo non resti una monade, aliena dalla realtà tecnologica che la circonda, bensì possa beneficiare – attraverso un bilanciamento «dei rischi connessi all'uso dei dispositivi *de quibus* rispetto alla congrua tutela delle prerogative individuali» – delle straordinarie potenzialità che, per certo, il progresso scientifico-informatico saprà offrire (anche grazie all'avvento dell'intelligenza artificiale) al rito penale[73]. D'altronde, «il progresso non può essere fermato, ma deve essere governato nel suo sviluppo; a tal fine è perciò, necessario realizzare un modello di processo penale tecnologicamente avanzato che tuteli le garanzie delle parti anche quando le stesse vengono declinate nei moderni territori digitali: questo deve essere il terreno di confronto, questo deve essere lo spirito profondo della digital transformation giudiziaria il cui futuro è solo nelle nostre mani, oggi più che mai»[74].

[72] J. Della Torre, *Algoritmi di facial recognition e procedimento penale italiano*, *op. cit.*, p. 178.

[73] D. Polidoro, *op. cit.*, p. 38.

[74] V. Bove, R. Patscot, *op. cit.*, p. 20.

G. Galluccio Mezio

TECNOLOGIE DI RICONOSCIMENTO FACCIALE: UNA RIFLESSIONE SUL LORO IMPIEGO CON FINALITÀ INVESTIGATIVE E PROBATORIE

1. *L'irresistibile ascesa delle tecnologie di riconoscimento del volto*

In via di prima approssimazione, le tecnologie di riconoscimento facciale possono essere definite come *software* che, attraverso processi informatici basati sull'impiego di algoritmi, consentono di stabilire – entro un certo margine di errore – la corrispondenza tra due immagini ritraenti il volto di una persona[2].

[1] Il presente contributo è stato redatto dall'Autore, in qualità di assegnista di ricerca presso il Dipartimento della Facoltà di Giurisprudenza dell'Università di Macerata, nell'ambito del progetto di ricerca "Il processo penale telematico tra efficienza e nuovi *vulnera* ai diritti dell'imputato". Il medesimo contributo, con l'autorizzazione della curatrice, è già stato pubblicato nella rivista Cassazione Penale, nel febbraio 2025.

[2] Per una analisi semplificata ma esaustiva dei meccanismi di concreto funzionamento di tali *software* nella letteratura processualpenalistica, si rinvia, tra molti, ad A. Marandola, *Il riconoscimento facciale*, in C. Conti (cur.), A. Marandola (cur.), *La prova scientifica,* Giuffrè, 2023, 500 ss.; nonché J. Della Torre, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.*, 2022, 41 ss. Per una disamina più ampia e diffusa, v. G. Mobilio, *Tecnologie di riconoscimento facciale (Rischi per i diritti fondamentali e sfide regolative)*, Editoriale Scientifica, 2021, 31 ss.

Il loro impiego costituisce un'abitudine quotidiana molto diffusa nelle società civili dei Paesi sviluppati.

Il progresso tecnologico e la diffusione dei dispositivi informatici ha condotto un'ampia porzione dell'umanità a ricorrere a tali applicativi nell'espletamento di processi di autenticazione e verifica dell'identità della persona abilitata ad accedere a sistemi informatici ad accesso controllato.

La gran parte dei moderni *smartphone* e dei sistemi di gestione da remoto dei rapporti bancari (cd. *home banking*) prevedono, ad esempio, tali modalità di verifica dell'identità dell'operatore.

Molti *social network* utilizzano programmi informatici di questo genere per offrire servizi agli utenti, agevolando l'identificazione di amici o conoscenti le cui immagini siano presenti nei relativi *database*.

Come dimostrano diverse esperienze straniere e nazionali, tali tecnologie (tanto nella funzionalità del riconoscimento cd. "uno a uno" che "uno a molti") vengono impiegate per consentire o negare l'accesso a edifici pubblici e privati, verificare le presenze degli studenti all'interno degli edifici scolastici, velocizzare i controlli ai valichi di frontiera, garantire l'accesso ai servizi pubblici[3].

[3] In argomento, *ex pluribus*, v. S. Del Gatto, *La* governance *delle nuove tecnologie tra tentativi di regolazione e istanze di* self regulation. *Il caso del riconoscimento facciale*, in *Riv. ital. dir. pubbl. comunitario*, 2023, 42 ss., la quale segnala come tecnologie di riconoscimento facciale risultino essere state impiegate negli più svariati campi e settori. In molti stati europei (come la Svezia e la Francia) ed extraeuropei, esse hanno applicazione nel campo dell'istruzione per controllare e monitorare l'accesso di studenti e visitatori e per individuare rapidamente potenziali rischi per la sicurezza degli studenti. L'impiego di tali tecnologie interessa anche i trasporti aerei, come avviene in alcune aree dell'aeroporto di Fiumicino, nonché in quello madrileno Adolfo Suarez Madrid – Barajas, con funzioni di controllo degli accessi a determinate aree dei rispettivi scali. Va, inoltre, ricordato il ricorso a simili tecnologie nel settore dei servizi di trasporto cittadini, per consentirne la fruizione senza necessità di presentazione del biglietto, come nel caso del sistema *Face Pay* attivo presso la metropolitana della città russa di Mosca, nonché dei sistemi di riconoscimento facciale attivi presso molte fermate degli autobus ed entrate ai treni di superficie nel territorio della Repubblica Popolare di Cina. Una menzione merita, altresì, l'impiego di tali tecnologie con finalità di verifica dei soggetti abilitati ad accedere ad edifici pubblici o privati. Tanto è avvenuto sia in Italia, dove risulta che videocamere munite di *termoscanner*, finalizzati alla rilevazione della temperatura dei passeggeri nell'ambito dell'attività di contenimento della pandemia da Covid-19 ma dotate, altresì, di sistemi di riconoscimento facciale, siano state istallate presso gli ingressi di Palazzo Chigi, sia nelle città statunitensi di Detroit e New York, dove analoghi strumenti risultano attivi per governare l'accesso a complessi residenziali pubblici. A ciò va aggiunto il ricorso ad analoghi strumenti per scopi di monitoraggio della sicurezza pubblica e stradale, che si ha no-

Nonostante l'opacità informativa che li caratterizza, si ha notizia che diversi Stati autoritari, specie all'indomani della diffusione di videocamere dotate di funzioni di rilevamento della temperatura corporea per il contenimento della pandemia da Covid-19, abbiano utilizzato o utilizzino tali strumenti (specie nella funzionalità "uno a molti") con scopi di sorveglianza di massa, di repressione del dissenso, di individuazione e identificazione di manifestanti la cui condotta è, nei rispettivi ordinamenti, incriminata ovvero costituisce titolo per l'attivazione di misure di polizia[4].

Si è, dunque, al cospetto di un ricorso estensivo a *software* di *facial recognition* sia per la gestione di rapporti privati sia per l'espletamento di funzioni pubbliche o di rilevanza pubblica.

È piuttosto agevole comprendere quali siano le potenzialità di tali strumenti nell'esercizio di funzioni di polizia amministrativa e giudiziaria, come dimostrano alcune vicende giudiziarie straniere[5], nonché lo

tizia vengano impiegati nella città di New York, dove telecamere dotate di sistemi di riconoscimento facciale sarebbero in uso su numerosi ponti, viadotti e tunnel stradali. Estensivo ricorso al loro impiego si registra, inoltre, nel settore dell'erogazione di svariati servizi digitali, sia pubblici che privati, come sperimentato nella città di Singapore che si è dotata della tecnologia denominata *SingPass.* Lo stesso dicasi per il controllo delle frontiere, negli Stati Uniti, dove la *U.S. Customs and Border Protection* utilizza tali strumenti per controllare le persone che richiedono l'ammissione al territorio nazionale, nonché nell'area dell'Unione Europea, che ricorre a una tecnologia di riconoscimento facciale simile al *Biometric Exit Program* nei porti di ingresso per verificare l'identità delle persone che richiedono visto e asilo.

[4] Anche in questo caso, si rinvia, tra molti, a S. Del Gatto, *La* governance *delle nuove tecnologie*, cit., 47, nella parte in cui richiama il sistema cinese del cd. *social score*, nonché l'impiego di tecnologie di riconoscimento facciale, da parte delle autorità cinesi, nella repressione delle proteste di Hong Kong. In argomento, v., altresì, S. Del Gatto, *Il riconoscimento facciale. A che punto siamo?*, in *Giorn. dir. amm.*, 2022, 692 ss. Fonti giornalistiche e *report* di organizzazioni non governative con scopi di tutela dei diritti umani, danno notizia dell'impiego, da parte del Governo della Federazione Russia, di sistemi di riconoscimento facciale per l'individuazione dei dissidenti che partecipano a manifestazioni politiche ostili all'attuale regime. In tema, tra molte, *https://www.amnesty.org/en/latest/press-release/2021/04/russia-police-target-peaceful-protesters-identified-using-facial-recognition-technology/*.

[5] Si fa riferimento, in particolare, al caso gallese, esaminato da S. Del Gatto, *La* governance *delle nuove tecnologie*, cit., 50 ss.; e da A. Mascolo, *Riconoscimento facciale e autorità pubbliche*, in *Giorn. dir. amm.*, 2021, 311 ss.; nonché alla vicenda giudiziaria – esitata nella pronuncia della Corte Suprema del Wisconsin (State v. Loomis, 13 luglio 2016) – relativa all'impiego del sistema COMPAS (acronimo di *Correctional Offender Management Profiling for Alternative Sanctions*), un programma di giustizia elaborato da una società statunitense per calcolare il rischio di recidiva, impiegato in diverse giurisdizioni statunitensi per computare le probabilità di reiterazione dei reati nei due anni suc-

scandalo suscitato dalla scoperta del meccanismo di funzionamento dell'applicazione informatica prodotta e posta in commercio dalla società statunitense *Clearview A.I.*[6].

Ulteriore conferma di ciò, in ambito nazionale, si trae dallo sviluppo del *software* denominato SARI (acronimo di "sistema automatico di riconoscimento delle immagini") su iniziativa del Ministero dell'Interno, poi messo a disposizione delle autorità di polizia, nonché dal duplice intervento, nel 2018 con riferimento alla versione denominata SARI *Enterprise*[7], nel

cessivi al momento di irrogazione o espiazione della pena. In argomento si rinvia, tra molti, a L. Romanò, *Intelligenza artificiale come prova scientifica nel processo penale: una sfida tra* machine-generated evidence *e equo processo,* in G. Canzio (cur.), L. Luparia Donati (cur.), *Prova scientifica e processo penale*, Cedam, 2022, 933.

[6] Si tratta di vicenda, in anni recenti, assurta agli onori delle cronache grazie al successo riportato da un *best seller* di successo (nell'edizione in lingua italiana, K. HILL, *La tua faccia ci appartiene*, Orville Press, 2024) e agli interventi operati dalle autorità garanti della *privacy* in Europa e negli Stati Uniti. Come riportato, ancora, da S. Del Gatto, *La* governance *delle nuove tecnologie*, cit., 46, l'istruttoria condotta sul punto dal Garante per la *privacy* italiano ha consentito di accertare che i dati personali detenuti dalla società produttrice della relativa applicazione informatica, prevalentemente tratti dai *social network* e relativi a circa dieci miliardi di utenti in tutto il mondo, sono stati trattati illecitamente e in violazione della normativa interna ed europea di settore. All'esito dell'indagine, l'Autorità ha irrogato alla società Clear View A.I. una sanzione amministrativa di venti milioni di euro e ha, altresì, disposto la cancellazione dei dati relativi a persone residenti in Italia, vietando l'ulteriore raccolta e trattamento. In proposito, più diffusamente, C. Ramotti, *Il Garante per la privacy italiano sanziona Clearview A.I.*, pubblicato sull'Osservatorio sullo Stato Digitale, IRPA, e consultabile all'indirizzo *https://www.irpa.eu/il-garante-per-la-privacy-italiano-sanziona-clearview-a-i/*; nonché I. Neroni Rezende, *Facial recognition in police hands: assessing the "Clearview case" from a European perspective*, in *N. J. of Eur. Crim. L.*, 2020, 375 ss.

[7] Sul punto, tra molti, J. Della Torre, *Tecnologie di riconoscimento facciale*, cit., 1077 ss., il quale chiarisce che, attraverso l'impiego di SARI *Enterprise*, «le autorità di *law enforcement* sono messe in grado di ricercare (in meno di quindici secondi) l'identità di un volto, presente in un'immagine già acquisita agli atti, all'interno di una banca dati di grandi dimensioni, individuata nella piattaforma AFIS – SSA (*Automated Fingerprint Identification System*), ovvero il "sistema automatizzato di identificazione delle impronte digitali", integrato dal "sottosistema anagrafico". Si tratta di *database* preesistenti, le cui funzionalità sono state sviluppate e replicate all'interno di SARI, ove confluiscono le immagini di diverse categorie di individui oggetto di foto segnalazione (tra cui, a esempio, persone sottoposte alle indagini, oppure che non siano in grado di provare la loro identità, o, ancora, migranti), nonché le informazioni concernenti i loro dati anagrafici e biometrici». Come segnala lo stesso A., alla luce di quanto riportato in risposta a un'interrogazione parlamentare (n. 5-03482 Ceccanti, in Atti Camera, I Commissione permanente, 5 febbraio 2020, in *www.camera.it*, p. 61), all'inizio dell'anno 2020, nella banca dati AFIS

2021 in relazione a quella denominata SARI *Real Time*[8], dell'Autorità Garante dei Dati Personali.

È noto che, a differenza del sostanziale avallo di SARI *Enterprise* nel 2018[9], con parere reso nel 2021[10], la suddetta autorità abbia ritenuto SARI *Real Time* suscettivo di violare i diritti fondamentali delle persone coinvolte e abbia definito illecito il trattamento dei dati biometrici svolto da quest'ultimo applicativo, in quanto destituito di adeguata base normativa e non conforme alla normativa di settore.

A seguito di quest'ultima pronuncia, il legislatore ha introdotto una moratoria rispetto all'istallazione e all'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale, operanti attraverso l'uso di dati biometrici, in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati, sino all'entrata in vigore di una disciplina legislativa *ad hoc* e, comunque, sino alla data del 31 dicembre 2023 (d.l. 8 ottobre 2021, n. 139, conv. con mod. dalla l. 3 dicembre 2021, n. 205), termine poi prorogato, al 31 dicembre 2025 (d.l. 51/2023).

Meno noto è segnalare che, per lo meno nella fase investigativa e nell'ambito di procedimenti ancora in corso, vi sia traccia del ricorso a SARI *Enterprise* nell'espletamento di indagini da parte della polizia giu-

erano presenti 17.592.769 cartellini foto segnaletici, corrispondenti a 9.882.490 individui diversi, di cui 2.090.064 di nazionalità italiana.

[8] Come riportato, ancora, da J. Della Torre, *Tecnologie di riconoscimento facciale*, cit., 1078 ss., «viceversa, SARI *Real Time* consente di individuare in diretta i volti inquadrati dalle telecamere (fisse o mobili), collocate in luoghi specifici oggetto di osservazione e confrontarli con un *database* più ristretto di persone ricercate (la c.d. "*watch-list*"), la cui grandezza è al massimo di 10.000 volti. Il sistema può, più in particolare, essere installato direttamente nel luogo ove sorga l'esigenza di disporre di una tecnologia di riconoscimento facciale per coadiuvare le forze di polizia nella gestione dell'ordine e della sicurezza pubblica, o in relazione a specifiche esigenze investigative. Allorquando la macchina riscontri una corrispondenza, viene a generarsi un *alert*, in grado di richiamare l'attenzione dei funzionari, cui spetta, anche in questo caso, il compito di confermare il riconoscimento e di prendere i provvedimenti conseguenti».

[9] Il parere del Garante, intitolato *Sistema automatico di ricerca di un volto – 26 luglio 2018* [doc. web 9040256], è reperibile all'indirizzo: *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9040256*.

[10] Il parere del Garante, intitolato *Parere sul sistema Sari Real Time – 25 marzo 2021* [doc. web 9575877], è reperibile all'indirizzo: *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877*. In argomento, v. R. Lopez, *Videosorveglianza biometrica tramite riconoscimento facciale: parere negativo del Garante per la* privacy, in *Proc. pen. e giust.*, 2022, 798 ss.; nonché E. C. Raffiotta, M. Baroni, *Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*, in *BioLaw Journal – Riv. BioDir.*, 2022, 165 ss.

diziaria, pur non potendo – per ovvie ragioni – stimarsi la frequenza di tale impiego.

L'enorme impatto sulla vita civile e sull'economia dei Paesi sviluppati delle tecnologie informatiche basate su sistemi di "intelligenza artificiale", tra i quali vanno certamente inclusi quelli di riconoscimento automatizzato del volto[11], è testimoniato dalla recente entrata in vigore del Regolamento europeo n. 2024/1689/UE che ha inteso introdurre un'organica disciplina relativa all'immissione in commercio e all'impiego di tali ritrovati e che, anche attese le disposizioni intertemporali previste[12], incoraggia i legislatori dei singoli Stati Membri a valutare l'introduzione di disposizioni di maggior dettaglio[13].

Scopo del presente studio non è quello di esplorare le potenzialità di tali strumenti nell'accertamento dei reati o nell'individuazione dei loro responsabili (del resto, del tutto intuitive), né di ripercorrere la storia recente dell'applicazione di tali tecnologie nei più svariati ambiti della vita civile o del diritto pubblico.

L'obiettivo, invece, è proporre una riflessione sulle prospettive del loro impiego in seno al procedimento penale, al lume di un inquadra-

[11] È utile precisare che l'art. 3 n. 1 del citato regolamento definisce espressamente come sistema di intelligenza artificiale: «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali». Indicazione, alquanto ampia, che – evidentemente – include i sistemi di riconoscimento facciale, i quali, a seconda delle rispettive caratteristiche tecniche, possono rientrare in una delle tre categorie espressamente definite a mente dei successivi nn. 41, 42 e 43 della stessa disposizione di legge, secondo le quali: per sistema di identificazione biometrica remota, deve intendersi «un sistema di IA finalizzato all'identificazione di persone fisiche, senza il loro coinvolgimento attivo, tipicamente a distanza mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento» (n. 41); per sistema di identificazione biometrica remota in tempo reale, deve intendersi «un sistema di identificazione biometrica remota in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi, il quale comprende non solo le identificazioni istantanee, ma anche quelle che avvengono con brevi ritardi limitati al fine di evitare l'elusione» (n. 42); per sistema di identificazione biometrica remota a posteriori, deve intendersi «un sistema di identificazione biometrica remota diverso da un sistema di identificazione biometrica remota "in tempo reale"».

[12] L'art. 113 del citato regolamento prevede che le disposizioni in esso contenute si applichino a decorrere dal 2 agosto 2026, fatti salvi i capi I e II la cui decorrenza è anticipata alla data del 2 febbraio 2025, mentre le previsioni di cui all'art. 6, paragrafo 1, e i corrispondenti obblighi si applicano a decorrere dal successivo 2 agosto 2027.

[13] In argomento, v. meglio *infra, sub* 9.

mento sistematico della disciplina normativa e della giurisprudenza sul contiguo settore delle prove e delle indagini atipiche, tenuto conto della mancanza di un'apposita disciplina nazionale e della carenza di specifiche indicazioni giurisprudenziali in materia.

Proposito che, del resto, appare coerente e strettamente correlato con il serrato processo di transizione digitale che l'ordinamento penale sta affrontando alla luce delle più recenti riforme, le quali preludono a una sempre più accentuata "apertura" alle tecnologie digitali e informatiche nel compimento degli atti del procedimento. Percorso evolutivo che, da un lato, offre indubbie prospettive di snellimento, velocizzazione e semplificazione dei meccanismi procedurali in cui questo si sostanzia, ma, al contempo, dall'altro, presenta, non secondari rischi di erosione dei diritti fondamentali delle persone coinvolte.

2. *Indagini preliminari e giudizio*

Una chiave di lettura utile all'inquadramento giuridico degli strumenti di *facial recognition* in ambito penale è la distinzione tra la fase delle indagini preliminari e quella del giudizio, nel cui alveo trova collocazione l'istruzione probatoria.

La scelta di tale "lente" attraverso cui addentrarsi nel tema oggetto di analisi discende dal rilievo che le due fasi sono caratterizzate da una spiccata eterogeneità con riferimento al ricorso, nel primo caso, a strumenti di indagine, nel secondo, a mezzi di prova non disciplinati dalla legge, quale – almeno *prima facie* (cfr. meglio *infra*) – appare essere l'impiego di *software* di riconoscimento del volto.

Costituisce un rilievo ricorrente in giurisprudenza quello secondo cui la fase investigativa sarebbe caratterizzata dal principio della tendenziale atipicità degli strumenti investigativi impiegabili[14].

In tal senso milita il tenore letterale dell'art. 348 comma 2 c.p.p.

L'indicazione secondo la quale, nello svolgere le proprie funzioni, la polizia giudiziaria procede «fra l'altro» a espletare le attività successivamente annoverate è, infatti, generalmente intesa come punto di emersione normativa di un canone più generale, idoneo a garantire ampia libertà agli inquirenti nella ricerca degli elementi utili alla ricostruzione del fatto

[14] *Ex pluribus,* Cass., Sez. II, 25 novembre 2020, n. 34211; Cass., Sez. V, 19 febbraio 2014, n. 18997; Cass., Sez. II, 27 marzo 2008, n. 16818; Cass., Sez. II, 27 giugno 2007, n. 35612.

oggetto della notizia di reato e all'individuazione del responsabile. Rilievo che, ovviamente, non equivale a sostenere che, allorché la legge disciplini espressamente un determinato atto di indagine, tale modello legale possa essere aggirato o eluso, dovendosi ritenere la possibilità di condurre investigazioni atipiche rigidamente vincolata all'espletamento di attività non oggetto di previsione legislativa, diversamente dovendosi diagnosticare il compimento di una attività tipica in violazione delle norme di legge all'uopo previste[15].

Da ciò consegue sia l'impossibilità di ritenere le attività di polizia disciplinate dalla legge alla stregua di un *numerus clausus*, del resto piuttosto ristretto, non prevedendosi, al suo interno, tradizionali attività investigative come, ad esempio, il "pedinamento"[16]; sia l'esigenza di estendere il suddetto principio anche alle attività di indagine svolte, direttamente o per delega, dal pubblico ministero, non potendosi ritenere precluso al *dominus* delle indagini ciò che è pacificamente concesso alla sua *longa manus*[17].

Una simile conclusione non ha solo basi testuali.

Essa è, altresì, coerente con l'architettura sistematica dell'ordinamento processuale, quantomeno nella sua ispirazione originaria di modello sagomato sull'ideale accusatorio.

Se, infatti, le indagini preliminari costituiscono la fase che «non conta e non pesa»[18], in quanto in essa si svolgono attività non suscettive di precostituire le basi probatorie della decisione di merito, ma solo propedeu-

[15] In questo senso, tra molti, M. Nobili, *Diritti per la fase che "non conta e non pesa"*, in Id., *Scenari e trasformazioni del processo penale*, Cedam, 1998, 44., secondo il quale «in definitiva, anche nella fase preliminare, è vietato costruire fattispecie "parallele" e "sostitutive", rispetto a quelle dettate dalla legge, asserendo che si tratterebbe di accertamenti atipici ("non nominati")».

[16] La vasta casistica sviluppata in materia di indagini atipiche non consente una esaustiva trattazione in questa sede, limitandosi a ricordare come in questo novero siano pacificamente ricondotte una vasta congerie di attività, sia tradizionali che "tecnologiche", come il pedinamento, l'appostamento, il sopralluogo, la ripresa video, l'ascolto non costituente intercettazione, l'istallazione su vetture nella disponibilità di persone oggetto di "attenzioni investigative" di dispositivi idonei al tracciamento mediante cd. GPS. In argomento, si vedano, tra molte, Cass., Sez. VI, 9 marzo 2023, n. 15422; Cass., Sez. IV, 27 novembre 2012, n. 48279; Cass., Sez. I, 7 gennaio 2010, n. 9416; Cass., Sez. VI, 11 dicembre 2007, n. 15396.

[17] Per tutti, v. A. Camon, *Le indagini preliminari*, in A. Camon, M. Daniele, D. Negri, C. Cesari, M. L. Di Bitonto, P. P. Paulesu, *Fondamenti di procedura penale,* IV ed., 2023, 474.

[18] M. Nobili, *Diritti per la fase che "non conta e non pesa"*, cit., p. 34 ss.

tiche alle determinazioni del pubblico ministero in ordine all'esercizio dell'azione penale e preparatorie delle successive iniziative dibattimentali, è consequenziale ritenere la loro regolamentazione improntata a un sostanziale *laissez fair*, fatti salvi i necessari presidi dei diritti inviolabili delle persone coinvolte[19].

Detto altrimenti, è congeniale a siffatta ricostruzione sistematica della fase e all'impostazione ideologica sopra richiamata, che la legge processuale stabilisca che le indagini preliminari siano contraddistinte da un principio di tendenziale atipicità e non rigidamente limitate allo svolgimento degli atti della polizia giudiziaria e del pubblico ministero espressamente disciplinati dalla legge.

In senso diametralmente opposto si pone la questione con riferimento al giudizio, dominato dal principio del contraddittorio nella formazione della prova e dal connesso canone di legalità della stessa, oggetto di presidio sia a livello di disciplina ordinaria che costituzionale[20].

Non scalfisce ma, semmai, conforta la linearità sistematica e concettuale di tale impostazione il dettato dell'art. 189 c.p.p., il quale, nell'introdurre un "varco" all'ammissione in giudizio di prove «non disciplinate dalla legge», non solo ribadisce pur sempre il rapporto di regola ad eccezione in essere tra i mezzi tipici di prova e quelli che tali non sono[21], ma soprattutto assoggetta l'assunzione della prova innominata all'integrazione di specifiche condizioni e all'osservanza di uno specifico procedimento legale[22].

Lo confermano gli sforzi compiuti dalla dottrina nel tentativo di demarcare il confine tra prova atipica e prova cosiddetta irrituale[23], vale a

[19] Sul punto, v., tuttavia, la precisazione contenuta alla precedente nota n. 15.

[20] In argomento, per tutti, P. Ferrua, *Il "giusto processo"*, III ed., 2012, 83 ss.

[21] M. Nobili, *Diritti per la fase che "non conta e non pesa"*, cit., p. 43.

[22] M. Nobili, *Il nuovo "diritto delle prove" ed un rinnovato concetto di prova*, in *La legislazione penale*, 1989, 396; conformemente v. anche M. L. Di Bitonto, *Le riprese video domiciliari al vaglio delle Sezioni unite*, in *Cass. pen.*, 2006, 4372 ss.

[23] Sul punto, v. A. Camon, *Le prove*, in A. Camon, M. Daniele, D. Negri, C. Cesari, M. L. Di Bitonto, P. P. Paulesu, *Fondamenti di procedura penale, cit.*, 336, il quale osserva: «la scelta legislativa di non "chiudere" il sistema probatorio sulle sole esperienze conoscitive disciplinate merita apprezzamento. L'art. 189 crea tuttavia un rischio, ossia che vengano contrabbandate come atipiche prove raccolte secondo modalità diverse da quelle stabilite dalla legge: un rischio niente affatto remoto, come dimostra la giurisprudenza sulle ricognizioni "informali". È un punto su cui bisogna essere fermi: la prova formata violando la legge è tipica (infatti la legge la regola); non è necessariamente invalida, questo no, perché può darsi che la violazione non faccia scattare sanzioni; però la questione della validità o invalidità della prova raccolta in questo modo non può essere aggirata

dire la prova tipica assunta con modalità diverse da quelle normativamente previste, orientati a scongiurare il rischio che la clausola di "apertura alla modernità" contenuta nella disposizione di legge sopra citata possa tradursi in uno stratagemma volto a eludere o aggirare il canone di legalità della prova[24].

Nonostante sia piuttosto sconfortante osservare come la giurisprudenza abbia in molti casi – specie con riferimento al problema della ricognizione irrituale – intrapreso e percorso esattamente il sentiero osteggiato dalla dottrina, garantendo accesso al fascicolo del dibattimento, in guisa di prova atipica, a riconoscimenti informali di ogni sorta[25], non può che ribadirsi la correttezza sistematica e l'ortodossia concettuale dell'impostazione tradizionale che, come detto, postula la tendenziale tipicità dei mezzi di prova suscettivi di essere assunti nel corso del giudizio.

L'asimmetria appena segnalata tra la fase del dibattimento e quella delle indagini preliminari è la ragione per la quale si è ritenuto opportuno adottare tale *summa divisio* nella presente esposizione, soffermandosi prioritariamente sulle prospettive di impiego dei sistemi di riconoscimento facciale in ambito probatorio, per poi occuparsi delle sue possibili applicazioni nel corso delle indagini preliminari.

invocando impropriamente la categoria delle prove innominate». V. anche, O. Mazza, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Dir. pen. cont., Riv. Trim.,* 2013, 3, 8, secondo il quale «il primo criterio di ammissibilità di qualsiasi prova, compresa quella atipica, era allora ed è a maggior ragione oggi, dopo l'entrata in vigore dell'art. 111 comma 1 Cost., quello di escludere esperimenti conoscitivi vietati dalla legge, non solo nel senso di prove contrarie ad espressi divieti normativi […] ma anche di prove difformi rispetto al modello di una fattispecie tipica, quindi *irrituali*».

[24] Rischio, del resto, segnalato già al momento dell'introduzione del codice vigente, ad esempio, da M. Nobili, *La nuova procedura penale*, Clueb, 1989, 119.

[25] Nel senso che la dichiarazione testimoniale confermativa di un precedente riconoscimento fotografico, eseguito in fase di indagini, costituisca una prova atipica, tra molte, Cass., Sez. II, 7 maggio 2019, n. 20489; Sez. IV, 13 settembre 2017, n. 47262; Cass., Sez. V, 1 ottobre 2015, n. 6456. Nel senso che il riconoscimento dell'imputato, operato in aula dal testimone senza l'ossequio delle forme della ricognizione personale, costituisca una prova non disciplinata dalla legge legittimamente acquisibile, Cass., Sez. II, 31 marzo 2022, n. 23970; Cass., Sez. VI, 27 gennaio 2015, n. 12501; Cass., Sez. II, 10 gennaio 2006, n. 3635; Cass., Sez. IV, 27 maggio 2004, n. 34354. Per un'aperta critica di tale impostazione, conducente a sovrapporre e confondere i concetti di prova atipica e prova irrituale, tra molti, G. Illuminati, *Ammissione e acquisizione della prova nell'istruzione dibattimentale*, in P. Ferrua, F. M. Grifantini, G. Illuminati, R. Orlandi, *La prova nel dibattimento penale*, III ed., Giappichelli, 2007, 135 ss.

3. *Riconoscimento umano e artificiale*

È piuttosto scontato osservare che la principale finalità del ricorso alle tecnologie di *facial recognition* in ambito processuale sia quella di individuare o riconoscere una persona o, più precisamente, di associare il volto di una persona nota (in quanto già censita in un *database* o precisamente identificata) a quello riprodotto per immagine in un documento o atto di rilevanza probatoria.

Quale che sia l'obiettivo, nel caso concreto, perseguito dalla parte che di tale strumento intende servirsi (*in primis,* l'individuazione di un testimone, della persona offesa o del sospettato), tale attività è finalizzata all'ottenimento di un risultato di conoscenza sovrapponibile a quello perseguito, nel corso del dibattimento, attraverso la ricognizione personale prevista dagli artt. 213 c.p.p. ss.; con la doverosa precisazione che, in quest'ultimo caso, l'associazione tra due immagini è compiuta, per così dire, *in corpore vivo* dalla persona chiamata a effettuare il riconoscimento e non si limita all'osservazione e al confronto delle sole fattezze del volto della persona da individuarsi.

La prima difficoltà concettuale è, dunque, stabilire se il ricorso a *software* di riconoscimento facciale riproduca la corrispondente attività euristica compiuta dall'uomo e, nel contesto del processo dibattimentale, affidata al modello legale della ricognizione.

Dal punto di vista tecnico, risulta che gli applicativi di riconoscimento facciale si basino, come anticipato in premessa, sull'impiego di algoritmi all'interno di un sistema informatico e che tali algoritmi siano annoverabili quali strumenti di "intelligenza artificiale", in quanto sottoposti a processi di "allenamento" e progressivo affinamento dei meccanismi algebrico-informatici di cui si avvalgono per comparare e individuare (cd. *matching*) le corrispondenze tra le immagini facciali in comparazione.

La semplice evocazione del termine "intelligenza artificiale", ma anche il ricorso a concetti come le "reti neurali", a indicare l'infrastruttura *hardware* e *software* che governa tali applicativi, tendono a suggerire un accostamento tra i processi informatici svolti dalla macchina e quelli cognitivi, neurologici ed euristici di cui si avvale l'essere umano. Tanto da legittimare l'impressione che il *facial recognition*, basato su sistemi di *artificial intelligence*, altro non sia che una *species*, magari più evoluta in quanto affidata alla macchina anziché all'essere umano, della ricognizione personale disciplinata nel terzo libro del codice di rito.

Le cose, tuttavia, non stanno in questi termini e, anzi, il ricorso ai

parallelismi tra le capacità intellettive umane e quelle delle macchine rischia di risultare fuorviante, anche ai fini della presente disamina.

I meccanismi mnestici ed euristici, affinati attraverso il lungo processo evolutivo della specie umana, dipendono infatti da meccanismi biologici e neurologici non riproducibili dalle macchine, i cui progettisti e programmatori possono – al più – imitare ma in alcun modo replicare.

Il funzionamento dei sistemi *software* e *hardware* che gestiscono applicativi di riconoscimento facciale funzionano, infatti, su basi algebrico-matematiche e all'interno di sistemi artificiali di tipo digitale e informatico[26]. L'attività che essi svolgono, specie nel campo del riconoscimento delle immagini, rappresentano il portato di complesse associazioni statistiche di *pixel* e vengono sviluppati e "allenati" mediante il ricorso a grandissime quantità di dati (per lo più, immagini), estratti da *database* di notevoli dimensioni (*cd. big data*). Dati che i moderni *computers* sono in grado di "processare", trattare, confrontare ed elaborare poiché dotati di straordinarie capacità computazionali[27].

Al contrario, il cervello umano e la sua capacità di "riconoscere" delle immagini facciali dipende da processi intellettivi e neurologici basati sulle "euristiche" o sulla cosiddetta "logica del pollice", vale a dire meccanismi epistemici e cognitivi finalizzati ad assumere scelte in condizioni di incertezza, scarsità di dati e in carenza di capacità computazionali analoghe a quelle delle macchine[28].

È importante sottolineare come le abilità umane che entrano in gioco nel corso di un riconoscimento non dipendono né sono governate da regole matematiche e non presuppongono il preventivo immagazzinamento di una enorme moltitudine di dati, ma sono strettamente correlate all'esercizio di capacità intuitive, non suscettive di essere tradotte in termini algebrico-statistici.

Lo dimostra la capacità dei bambini, anche in tenerissima età, di distinguere e riconoscere persone, oggetti e animali visti un numero molto limitato di volte e senza aver prima potuto visionare e consultare un elevato numero di immagini analoghe, né averle memorizzate[29].

La spiegazione di tale fenomeno è, con ogni probabilità, da ricon-

[26] In argomento, v. G. Ubertis, *Processo penale telematico, intelligenza artificiale e costituzione*, in *Cass. Pen.*, 2024, 439 ss.

[27] In argomento, per tutti, G. Gigerenzer, *Perché l'intelligenza umana batte ancora gli algoritmi*, Raffaello Cortina Editore, 2022, 102.

[28] G. Gigerenzer, *Perché l'intelligenza umana batte ancora gli algoritmi*, cit., 119 ss.

[29] G. Gigerenzer, *Perché l'intelligenza umana batte ancora gli algoritmi*, cit., 129 ss.

dursi al fatto che il bambino, come qualsiasi essere umano – a differenza della macchina – disponga del "concetto mentale" dell'oggetto che riconosce, quale che esso sia; di tal che è in grado di associarne l'immagine senza necessariamente averlo visto molte volte, lasciandosi condizionare anche dal contesto in cui è chiamato a esprimere il proprio giudizio[30]. Al contrario della macchina, non deve, infatti, basare le proprie valutazioni sull'associazione statistica dei *pixel* tra l'immagine da riconoscere e quelle già conosciute e presenti nel proprio "*database*" o nella propria memoria.

Si tratta di una caratteristica che sarebbe stata affinata nel corso dei secoli delle società umane al fine di consentire all'*homo sapiens* di compiere, nelle situazioni di incertezza tipiche del mondo reale, scelte "soddisfacenti", rapide e, dunque, "vincenti" da una prospettiva evoluzionistica, senza necessità di un impegno di capacità computazionali analoghe a quelle dei moderni microprocessori[31].

Tali considerazioni, pur appartenenti al dominio della epistemologia e delle *digital sciences*, dunque estranee alla cultura dell'operatore del diritto, rivestono un significativo rilievo se rapportate ai comuni criteri di decodificazione del fenomeno probatorio e delle sue regole.

Provando a ricondurle alle categorie più consuete per gli studiosi di procedura penale, si può con una certa sicurezza affermare che l'estrazione del dato di conoscenza rilevante in ambito processuale segue, nell'uomo e nella macchina, processi radicalmente differenti[32].

[30] G. Gigerenzer, *Perché l'intelligenza umana batte ancora gli algoritmi*, cit., 100 ss., il quale cita un recente studio che si è occupato, tra l'altro, di comparare le capacità del *computer* e del bambino di riconoscere un oggetto di comune esperienza, quale uno scuolabus.

[31] In ordine ai meccanismi intellettivi, selezionati dall'evoluzione, che consentono di assumere decisioni "efficienti" in situazioni di incertezza, in carenza di informazioni e in assenza di conoscenze e capacità computazionali analoghe a quelle dei moderni *computer*, v. G. Gigerenzer, *Decisioni intuitive,* Raffaello Cortina Editore, 2009, 8 ss.

[32] Una conferma di quanto affermato nel corpo del testo può trarsi persino dalla comparazione tra i processi cognitivi che soprassiedono alle scelte compiute dall'uomo e dalla macchina nel gioco degli scacchi, vale a dire nell'ambito di un sistema disciplinato da regole stabili e da un numero finito di combinazioni possibili (cd. principio del mondo stabile), dunque in un "ambiente" nel quale i moderni *computer* danno il meglio di sé e hanno, pacificamente, superato le capacità di gioco degli umani. Come autorevolmente sottolineato e sperimentalmente accertato, persino in un simile contesto, ontologicamente diverso dalle situazioni di incertezza e variabilità che, invece, contraddistinguono il mondo reale, le strategie di gioco adottate dall'uomo e dalla macchina si sono dimostrate *qualitativamente* diverse. I moderni sistemi *software* progettati per il gioco degli scacchi

Per risalire al dato ignoto (la corrispondenza o meno del volto) a partire da un dato noto (le due o più immagini poste in comparazione) il cervello umano ricorre a meccanismi molto complessi e, in molti casi, ancora sconosciuti ma, indubbiamente, eterogenei rispetto a quelli della macchina.

Quest'ultima impiega in maniera automatizzata un coacervo leggi scientifiche – quelle che governano la matematica, la statistica, l'informatica, l'intelligenza artificiale – che solo un sistema artificiale dotato di elevatissime capacità di calcolo è in grado di governare.

Nessuna di esse è, però, alla base del meccanismo euristico che consente all'essere umano di esprimere un giudizio di corrispondenza tra due persone (dunque, di riconoscerle), sia tale giudizio il portato di una visione *live* o sia esso il risultato di una comparazione avvenuta mediante la semplice visione e il confronto di due immagini.

Al di là delle suggestioni evocate dal ricorso a terminologie più o meno accattivanti, occorre, dunque, concludere che l'attività epistemica condotta, in maniera automatizzata, dai *software* di riconoscimento facciale non sia in alcun modo accostabile al riconoscimento compiuto dall'uomo.

Questi programmi, così come tutti gli applicativi basati sulla cd. "intelligenza artificiale", tendono a riprodurre e velocizzare funzioni del cervello umano, ma non ne replicano – per quante somiglianze si possano ravvisare tra di esse – i processi e i meccanismi di funzionamento.

Il riconoscimento facciale operato da un *computer* non è, allora, attività in alcun modo sovrapponibile né accostabile alla ricognizione personale disciplinata dall'art. 213 c.p.p.: non soltanto perché essa risulta compiuta da una macchina anziché da un essere umano; ma, altresì, perché è condotta attraverso processi di trattamento, elaborazione e combinazione dei dati oggettivamente eterogenei da quelli che entrano in gioco nel corso della ricognizione disciplinata dalla legge[33].

come, ad esempio, Deep Blue (che ha dimostrato di poter battere qualsiasi giocatore umano) utilizzano, infatti, «la forza bruta della [loro] potenza combinatoria», mentre lo scacchista ricorre non solo alla capacità di prevedere mentalmente le mosse successive (molto inferiore a quella della macchina) ma alla capacità di riconoscere «le configurazioni spaziali» dei pezzi posti sulla scacchiera, a significare che le strategie impiegate dall'uomo per il compimento di scelte condizionate dalla impossibilità di operare calcoli particolarmente complessi presentino irriducibili diversità qualitative rispetto a quelle affidate alla potenza computazionale dei moderni sistemi di "intelligenza artificiale". In tal senso, G. GIGERENZER, *Decisioni intuitive,* cit., 65 ss.

[33] Affermazione che è, peraltro, empiricamente confermata dalla circostanza che an-

Non si è, pertanto, dinanzi a una "ricognizione operata dalla macchina" anziché dall'uomo, perché l'attività cognitiva e epistemologica rilevante è condotta da una "entità" che non soltanto non ha sembianze antropomorfe ma, soprattutto, "ragiona", elabora i dati di cui dispone e perviene a dei "risultati" attraverso processi, oggettivamente, diversi da quelli umani.

Si tratta, dunque, di una "prova" che, neppure in senso lato, può ritenersi disciplinata dalla legge, né suscettiva di essere sovrapposta al modello tipico previsto dagli artt. 213 ss. c.p.p.

4. *Prova atipica o prova tipica basata su una* novel science?

L'impossibilità di ricondurre le tecnologie di *facial recognition* al modello della ricognizione non risolve del tutto la questione se esse debbano qualificarsi alla stregua di prova non disciplinata dalla legge a mente dell'art. 189 c.p.p.

Occorre, infatti, domandarsi se i risultati di conoscenza discendenti dal loro impiego possano essere veicolati in giudizio attraverso mezzi di prova tipici, quali la consulenza tecnica o la perizia.

In tal senso potrebbe militare il rilievo che tali ritrovati tecnologici rientrino nel campo della cd. nuova prova scientifica[34].

che la tipologia di errori, nel riconoscimento delle immagini come nel compimento di altro tipo di attività, commessi dall'uomo e dalla macchina differiscono in maniera estremamente marcata. Sul punto si rinvia, ancora una volta, a G. Gigerenzer, *Perché l'intelligenza umana batte ancora gli algoritmi*, cit., 132 ss.: «Se un sistema è un miglioramento di un altro, commette meno errori – ma tipicamente si tratta di errori dello stesso tipo. Tuttavia, se due sistemi differiscono nelle loro proprietà fondamentali, come il carbonio e il silicio, è probabile che commettano errori qualitativamente diversi. Quindi, se le reti neurali artificiali fossero simili all'intelligenza umana, gli errori che commettono dovrebbero differire in termini di quantità. Invece differiscono nella qualità. Una differenza qualitativa è un errore dell'IA che sia inatteso e non intuitivo per un umano, o un errore umano che l'IA non commetterebbe mai». Rilievo che, peraltro, consente di comprendere come la possibilità dell'uomo di identificare gli errori commessi dalla macchina sia particolarmente complicata dal loro carattere, fondamentalmente, contro intuitivo, con implicazioni – anche nel settore dell'applicazione processuale di tali strumenti – di tutta evidenza.

[34] Per un'ampia e articolata definizione del concetto di prova scientifica, per tutti, O. Dominioni, *La prova penale scientifica (Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione)*, Giuffrè, 2005, 12 ss. In ordine al concetto di *novel science*, pare sufficiente, ai limitati fini della presente disamina, ricordare come la dottrina sia so-

Non c'è, infatti, dubbio che i *software* di riconoscimento facciale operino sulla scorta di leggi scientifiche (la matematica, l'algebra, la statistica) ma soprattutto di discipline (come l'informatica e l'intelligenza artificiale) di recente sviluppo e di ancor più recente impiego nell'ambito del processo penale.

In analogia con quanto avvenuto per altre discipline forensi[35] e alla luce di quanto sostenuto dalla dottrina, ad esempio, nel caso delle neuroscienze[36], si potrebbe pertanto essere indotti a collocare il loro impiego nell'alveo degli accertamenti o delle valutazioni esperte disciplinati dagli artt. 220 ss. c.p.p.[37].

Si tratta, tuttavia, di un abbaglio foriero di insidiose applicazioni.

Se infatti, con ragionevole grado di certezza, il ricorso a tali strumenti deve inquadrarsi nel campo della prova scientifica basata su una *novel science*[38], ciò non implica che essa debba essere qualificata né veicolata attraverso le forme della perizia o della consulenza tecnica.

Come già rilevato, l'attività epistemologica che consente di estrarre la

stanzialmente concorde nel distinguere due categorie concettuali: i mezzi di prova che implicano l'impiego di metodiche analitiche o conoscenze condivise nella comunità scientifica e sociale di riferimento ovvero di collaudato e frequente impiego in ambito giudiziario e quelli rientranti nella categoria della cosiddetta "prova scientifica nuova"; con quest'ultima espressione dovendosi intendere gli strumenti tecnico-scientifici totalmente nuovi o controversi e di elevata specializzazione, annoverati dalla letteratura giuridica di lingua inglese alla stregua di *novel sciences*. In tal senso, tra molti, G. Ubertis, *Prova scientifica e processo penale*, in *Riv. it. dir. proc. pen.*, 2016, 1193 ss.; nonché O. Dominioni, *La prova penale scientifica*, cit., 13 ss.

[35] È questo il caso, ad esempio, della cd. *Blood Pattern Analysis*, ossia l'analisi delle tracce ematiche, come riconosciuto finanche da Cass., Sez. I, 21 maggio 2008, n. 31456 in *Cass. pen.*, 2009, 1867 con nota di F. Caprioli, Scientific evidence *e logiche del probabile nel processo per il "delitto di Cogne"*.

[36] Sul punto, per tutti, v. P. Ferrua, *La prova nel processo penale (struttura e procedimento)*, vol. I, Giappichelli, 2015, 278; al riguardo è, però, utile menzionare, altresì, l'opinione di O. Mazza, *I diritti fondamentali dell'individuo come limite della prova*, cit., p. 8, secondo cui «non esiste, ad esempio, una prova scientifica non sussumibile nei collaudati schemi normativi della prova tecnica».

[37] Prospetta un simile inquadramento della prova fondata sull'applicazione di sistemi di intelligenza artificiale, pur riconoscendo che «la prova algoritmica, per sua natura, è diversa da quella scientifica in quanto chi la offre non è un umano ma una IA, che lo fa sulla base di *input* e processi automatizzati non immediatamente intellegibili per la persona comune», L. Romanò, *Intelligenza artificiale come prova scientifica nel processo penale*, cit., p. 928.

[38] Nel senso che la prova acquisita mediante applicazione di tecnologie informatiche e digitali sia inquadrabile in una *species* del *genus* della prova scientifica, tra molti, L. Marafioti, Digital evidence *e processo penale*, in *Cass. Pen.*, 2011, 4510; nonché M. Gia-

conclusione probatoria dai dati o dalle immagini disponibili è, infatti, compiuta interamente dalla macchina e non da un essere umano, per quanto culturalmente o tecnicamente attrezzato, e avviene alla stregua di processi algoritmici del tutto eterogenei e non sovrapponibili al funzionamento dell'intelletto umano.

L'intervento di un soggetto esperto che adopera la macchina non rende, per ciò solo, tale valutazione ascrivibile al primo, ben potendo una eventuale perizia o consulenza tecnica essere introdotta quale ausilio alla comprensione e alla "lettura" del risultato offerto dal *software* ma, in nessun caso, potendosi confondere la natura e il regime giuridico dei due diversi e, semmai, complementari mezzi di prova.

Lo stesso dicasi anche nel caso in cui lo specifico applicativo di *facial recognition* impiegato nel caso concreto sia contraddistinto da modalità di funzionamento analoghe a quello conosciuto come SARI *Enterprise*, attualmente in uso alle forze di polizia.

Com'è noto e in analogia al meccanismo di funzionamento del sistema AFIS, che opera attraverso la comparazione automatizzata delle impronte digitali immagazzinate nell'omonima banca dati, tale *software* restituisce una serie di possibili accoppiamenti (*machting*) tra l'immagine in verifica e quelle già presenti in banca dati, unitamente a una percentuale di corrispondenza, lasciando all'operatore umano il compito di confermare o smentire il risultato, in ossequio al principio *human in the loop,* di frequente applicazione in materia di *artificial intelligence*.

Anche in questo caso si è, infatti, dinanzi a due fonti informative eterogenee e, dunque, meritevoli di diversa e autonoma disciplina: la prima consiste in un giudizio di compatibilità, appannaggio esclusivamente della macchina; la seconda in una supervisione umana del risultato offerto dalla macchina, sulla scorta di competenze più o meno sviluppate da parte del soggetto incaricato.

Attività di supervisione che, però e con ogni evidenza, non trasforma in un giudizio umano o in una valutazione esperta un processo di trattamento ed elaborazione di dati biometrici compiuto dal sistema di *facial recognition* e non altera, dunque, l'ontologica atipicità del mezzo di prova impiegato.

Lo conferma – del resto – l'impossibilità di un simile meccanismo di prevenire o scongiurare il rischio del cosiddetto "falso negativo", non essendo sottoposti al giudizio umano gli accoppiamenti, per così dire,

LUZ, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA. VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Giuffrè, 2021, 51 ss.

"scartati" dalla macchina ma solo quelli positivamente rilevati, sia pure alla stregua di un determinato coefficiente di probabilità.

Ne consegue che, qualunque sia il meccanismo concreto di funzionamento del singolo applicativo di riconoscimento facciale, può, con buona approssimazione, ritenersi tali tecnologie senz'altro ricadenti nell'alveo applicativo dell'art. 189 c.p.p. e, dunque, sottoposte ai limiti di ammissibilità stabiliti da questa disposizione di legge[39].

5. *La dubbia idoneità epistemologica e validità scientifica delle tecnologie di* facial recognition *in ambito probatorio*

L'inquadramento appena proposto dei sistemi di *facial recognition* induce a segnalare un primo, significativo, ostacolo alla loro ammissibilità probatoria.

Come già osservato, il loro meccanismo di funzionamento si basa sull'impiego di leggi scientifiche e, soprattutto, di discipline tecniche prive di un consolidato accreditamento in ambito processuale. Rilievo che, per ovvie ragioni, è da intendersi specificamente riferito alla branca dell'informatica indicata come "intelligenza artificiale" e, all'interno di essa, agli algoritmi che soprassiedono al riconoscimento automatizzato dei volti.

Non si ravvisa, del resto, nella giurisprudenza una "storia" di applicazione giudiziaria di tali congegni.

Occorre, dunque e in primo luogo, stabilire se tali tecnologie risultino idonee – sotto il profilo conoscitivo – all'accertamento dei fatti, come postula l'art. 189 c.p.p. nell'attribuire al giudice dibattimentale il compito di una verifica preliminare in ordine alla «idoneità epistemologica»[40] e alla «validità scientifica»[41] del mezzo di prova oggetto della richiesta di parte.

Com'è noto, l'eco della giurisprudenza statunitense (dalla sentenza *Frye* alla sentenza *Daubert*) ha esplicato una notevole influenza sulla giu-

[39] In tal senso, A. Marandola, *Il riconoscimento facciale*, cit., 511 ss.; J. Della Torre, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1082 ss.; M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. proc.*, 2021, 1052; G. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte euro unitario*, in *La legislazione penale*, 2021, 9.

[40] G. Ubertis, *Prova scientifica e processo penale*, in *Riv. it. dir. proc. pen.*, 2016, 1201.

[41] M. Taruffo, *La prova scientifica. Cenni generali*, in *Ragion pratica*, 2016, 343.

risprudenza interna che si è incaricata di codificare i criteri utili alla risoluzione di un simile quesito e, soprattutto, di chiarire i margini dell'apprezzamento del giudice in ordine alla richiesta di parte finalizzata all'introduzione di una prova basata su una *novel science*[42].

È del resto pressante l'esigenza di scongiurare l'ingresso, tra le prove utili alla decisione di merito, a quella che viene comunemente definita come *junk science* o "scienza spazzatura", rappresentata da metodologie e da tesi carenti di rigore logico e, soprattutto, prive di effettiva valenza scientifica[43]. Com'è stato autorevolmente sottolineato, tuttavia, non sempre è «agevole individuare l'ideale spartiacque tra effettivi "esperti" e semplici "millantatori", tra contributi "scientifici" ed opere "pseudo-scientifiche"»[44].

Tale profilo dei rapporti tra scienza e processo è altamente problematico, anche perché strettamente intrecciato all'apparente paradosso del giudice inesperto che è tenuto a giudicare l'operato dell'esperto o, comunque, la validità gnoseologica di discipline a lui sconosciute[45]. Ragion per cui si è fatta strada una concezione del giudice che, sottraendosi all'anacronistico (e, per molti versi, fuorviante) ideale dello *iudex peritus peritorum*[46], ne esalta la funzione di garante della accuratezza del metodo di

[42] Per un'ampia panoramica del percorso compiuto dalla giurisprudenza straniera e da quella interna sul punto, v. G. Gennari, *I criteri di ammissione della prova scientifica nel contesto internazionale*, in G. Canzio (cur.), L. Luparia Donati (cur.), *Prova scientifica e processo penale*, cit., 157 ss.

[43] Al riguardo, per tutti, appare utile richiamare le osservazioni di O. Dominioni, *In tema di nuova prova scientifica*, in *Dir. pen. proc.*, 2001, 1062, il quale non manca di evidenziare come una stringente esigenza sia quella di evitare che «il processo sia inquinato dall'abuso della prova scientifica, proteggendolo cioè dalla cattiva scienza (*junk science* o *bad science*): principi e metodi non validi, esperti partigiani, operazioni tecniche non controllabili nella loro correttezza, strumenti scientifico-tecnici» che tendano a «creare confusione nel giudice del fatto, a creare suggestioni e pregiudizi nel nome di una mitica infallibilità della scienza e della tecnica, a risultare tanto sofisticati quanto incomprensibili, a non avere un nesso con il *thema probandum*, a nuocere all'economia del processo […]». Istanze che, per converso, devono fare il paio con l'altrettanto importante esigenza che l'accertamento processuale non rinunci alla possibilità di avvalersi di impostazioni e metodiche scientifiche fortemente innovative che avrebbero «il solo "torto" di porsi in antagonismo con le opinioni consolidate di buona parte del mondo accademico in un determinato momento storico». Così P. Rivello, *Tecniche scientifiche e processo penale*, in *Cass. pen.*, 2013, 1693.

[44] P. Rivello, *Tecniche scientifiche e processo penale*, cit., 1693.

[45] In argomento, per tutti, M. Taruffo, *Scienza e processo,* XXI Secolo, Treccani, 2009; nonché, O. Dominioni, *La prova penale scientifica*, cit., 67 ss.

[46] In tal senso, O. Dominioni, *L'esperienza italiana di impiego della prova scientifica nel processo penale*, in *Dir. pen. proc.*, 604.

accertamento dei fatti oggetto di giudizio[47]. Sfornito di competenze specialistiche nelle più disparate branche del sapere, ma munito di una «cultura dei criteri»[48], egli sarebbe, perciò, in grado di esercitare quella funzione di «*gatekeeper*, di guardiano che previene l'introduzione nel processo della cosiddetta scienza spazzatura»[49]. Tanto alla stregua di una impostazione concettuale che non soltanto appare sufficientemente condivisa ma, soprattutto, l'unica in grado di contemperare l'esigenza di sottrarre il giudice dalle più disparate dispute scientifiche o nomologiche e, contestualmente, richiamarlo al ruolo di garante dell'igiene processuale e della correttezza epistemologica del metodo seguito per la ricostruzione dei fatti.

Va, del resto, preso atto che costui, non essendo produttore ma mero fruitore di leggi scientifiche, «non può appropriarsi della "competenza" dello scienziato e tuttavia non deve essere un fruitore passivo; la sua "competenza" non declinabile è di vagliarne l'affidabilità nell'uso probatorio»[50].

In definitiva, non può essere richiesto al giudice di possedere le nozioni specialistiche e tecnico-scientifiche appannaggio dello scienziato o dell'esperto, mentre è certamente tenuto e, in questo senso, responsabilizzato[51] a disporre delle nozioni di metodo e delle conoscenze epistemologiche che gli consentano di stabilire la validità scientifica della prova ai fini dell'accertamento del fatto[52].

[47] *Ex pluribus,* C. Conti, *Scienza controversa e processo penale: la Cassazione e il "discorso sul metodo"*, in *Dir. Pen. Proc.*, 2019, 848.

[48] O. Dominioni, *La prova penale scientifica*, cit., 69.

[49] G. Ubertis, *Prova scientifica e processo penale*, cit., 1202.

[50] O. Dominioni, *L'esperienza italiana di impiego della prova scientifica nel processo penale*, cit., 603.

[51] Al riguardo, v. S. Lorusso, *Il contributo degli esperti alla formazione del convincimento giudiziale*, in *Archivio pen.*, 2011, 2, il quale rileva il rischio di una «deresponsabilizzazione cognitiva del giudice cui fa da *pendant* la figura dell'esperto a sua volta deresponsabilizzato dall'inaccessibilità del sapere di cui è (o si presume sia) depositario».

[52] Per tutti, M. Taruffo, *La prova scientifica*, cit., 348, secondo il quale «ciò di cui il giudice ha bisogno per effettuare le sue valutazioni sulla prova scientifica sono le nozioni *di metodo* e le conoscenze *epistemologiche* che occorrono per compiere effettivamente i controlli di cui si è parlato. Se il giudice non dispone di queste nozioni la sua funzione di *peritus peritorum* risulta completamente svuotata: l'unico vero *peritus* rimane l'esperto, alla cui opinione il giudice presta un assenso acritico o sulla quale formula un dissenso altrettanto acritico». Analogamente, L. De Cataldo Neuburger, *Il diritto, la perizia e il sapere "altro"*, in L. De Cataldo Neuburger (cur.), *Scienza e processo penale*, Cedam, 2010, 242.

Sussiste, del resto, un generalizzato consenso in ordine ai criteri, principalmente mutuati dalla giurisprudenza statunitense[53], che soprassiedono all'espletamento di tale operazione e possono essere riassunti come segue: la possibilità di stima del margine di errore connesso all'impiego della *novel science*; la controllabilità e falsificabilità (in senso popperiano) della teoria; la pubblicazione degli studi e delle ricerche impiegati nella lettura specialistica e, in particolare, in riviste soggette a revisione; il grado di accettazione di tale metodo di ricostruzione dei fatti da parte della comunità scientifica di riferimento; la rilevanza specifica del metodo di accertamento e delle conoscenze acquisibili rispetto ai fatti di causa[54].

Si tratta di canoni che, sebbene con sfaccettature e accentuazioni diverse, sono stati – nei fatti – "tradotti" e, dunque, "recepiti" dal diritto vivente, che ha inteso trasformare il cosiddetto *Daubert test* «in un obbligo di motivazione rafforzata cui il giudice può adempiere esclusivamente se ha attivato un previo contraddittorio su alcuni profili imprescindibili al fine di sondare efficacemente la qualità del sapere scientifico introdotto nel processo»[55].

[53] In argomento, diffusamente, O. Dominioni, *La prova penale scientifica*, cit., 115 s.; F. Caprioli, Scientific evidence *e logiche del probabile nel processo per il "delitto di Cogne"*, in *Cass. pen.*, 2009, 1869; P. Rivello, *La prova scientifica*, Giuffrè, Milano, 2014, 66 ss.; G. Ubertis, *Prova scientifica e processo penale*, in *Riv. it. dir. proc. pen.*, 2016, 1202; nonché P. Tonini, *La Cassazione accoglie i criteri Daubert sulla prova scientifica. Riflessi sulla verifica delle massime di esperienza*, in *Dir. pen. proc.*, 2011, 1341 ss.; I riferimenti al *case law* statunitense sono essenzialmente alla triade costituita dalle notissime decisioni: Court of Appeals of District of Columbia, 3 dicembre 1923, n. 293, Frye v. United States, in *Federal Reporter*, 1923, 1013 ss.; Supreme Court of the United States, 28 giugno 1993, Daubert e a. v. Merrel Dow Pharmaceuticals, Inc., in *Minnesota Law Review*, 1994, 1345 ss.; Supreme Court of the United States, 23 marzo 1999, Kumho Tire Company Ltd. V. Carmichael, in 23, *The University of New South Wales Law Journal*, 1, 2000, 38 ss.

[54] In tal senso, sia pure con diverse accentuazioni, M. Taruffo, *La prova scientifica*, cit., 338; M. Bargis, *Note in tema di prova scientifica nel processo penale*, in *Riv. dir. proc.*, 2011, 51; C. Conti, *Scienza e processo penale*, in C. Conti (cur.), *Scienza e processo penale*, cit., 161; C. Intrieri, *Oltre ogni ragionevole dubbio o dell'utopia. Il caso Sally Clarck e "l'errore da pubblico ministero" (*the prosecutor's fallacy*)*, in L. De Cataldo Neuburger (cur.), *Scienza e processo penale*, cit., p. 291.

[55] C. Conti, *Scienza controversa*, cit., 850; contributo cui si rinvia anche per una sintetica ma esaustiva disamina dell'orientamento che si richiama nel corpo del testo. Per i riferimenti giurisprudenziali essenziali, v. Cass., Sez. IV, 17 settembre 2010, n. 43786, Cozzini e altri, in *Cass. pen.,* 2011, 1701; Cass., Sez. IV, 29 gennaio 2013, n. 16237, Cantore; Cass., 27 marzo 2015, n. 36080, Sollecito; Cass., sez. IV, 3 novembre 2016, n. 12175, Bordogna; Cass., sez. IV, 14 novembre 2017, n. 16715, Cirocco. In ordine alla maggior

Rapportando questi insegnamenti al caso dei sistemi di *facial recognition*, è piuttosto agevole concludere nel senso che essi ben difficilmente possano ritenersi idonei a soddisfare i suddetti criteri, poiché contraddistinti da un notevole tasso di «opacità algoritmica»[56].

Allo stato delle conoscenze disponibili, non sono infatti noti gli algoritmi concretamente impiegati, in quanto – in massima parte – sottoposti a segreto industriale e non resi disponibili dai loro titolari.

Neppure sono noti i meccanismi di "allenamento", tipici degli applicativi di *artificial intelligence,* di tali *software* e, in molti casi, non è neppure chiaro se i loro programmatori, in ragione delle operazioni di automatica riscrittura del codice informatico su cui essi si basano (cd. *machine learning*), possano ricostruire, passo per passo, il processo algoritmico ed epistemico impiegato per pervenire al singolo *match* o accoppiamento[57].

Grande incertezza sussiste, inoltre, sui tassi di errore (sia in termini di falso positivo che di falso negativo) che i singoli sistemi presentano, tenuto conto che i *trial* eseguiti per testarne l'affidabilità tendono ad essere svolti mediante la comparazione di immagini scattate in condizioni relativamente stabili o standardizzate e, dunque, certamente diverse da quelle presenti sulla scena di un crimine e, più in generale, tipiche del mondo reale.

Si tratta di preoccupazioni che, peraltro, hanno avuto vasta eco, finanche, nelle cronache, per esempio in occasione del conclamato fallimento dell'applicazione di sistemi di riconoscimento facciale a scopo di controllo dell'ordine pubblico e repressione dei reati commessi nell'oc-

complessità e ampiezza dei criteri e del metodo elaborati dalla sentenza Cozzini rispetto a quelli racchiusi nel cosiddetto *Daubert test*, v., A. Farano, *Scienza moderna e valutazione della prova scientifica*, in *Riv. dir. proc.*, 2021, 150 ss.

[56] Concetto richiamato e ribadito, in maniera pressoché unanime, da tutta la dottrina, tra cui, senza pretesa di esaustività, L. Luparia Donati, *Intelligenza artificiale e libero convincimento del giudice,* in G. Canzio (cur.), L. Luparia Donati (cur.), *Prova scientifica e processo penale*, cit., 944; F. Palmiotto, *The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in M. Ebers (cur.), M. Cantero Gamito (cur.), *Algorithmic governance and governante of algorithms,* Cham, 2021, 49 ss.; J. Danaher, *Algorithmic decision-making and the problem of opacità*, in *Comput. Law*, 2016, 8, 29. Sul tema specifico del ricorso in ambito probatorio a sistemi di riconoscimento facciale, A. Marandola, *Il riconoscimento facciale*, cit., 511 ss.; J. Della Torre, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1082 ss.; M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, cit., 1053 ss.

[57] Sottolinea, tra gli altri, esattamente tale profilo problematico, G. Ubertis, *Processo penale telematico, intelligenza artificiale e costituzione*, cit., 443.

casione di manifestazioni sportive, in particolare, mediante l'impiego della funzionalità di ricerca cd. "uno a molti"[58].

Né può trascurarsi di rilevare come, anche nell'esperienza quotidiana di impiego della funzionalità di ricerca "uno a uno", in uso sui comuni *smartphone* in commercio, finalizzata allo "sblocco" del dispositivo, sovente si assista a falliti riconoscimenti (che altro non sono che "falsi negativi") seguiti dall'invito a ripetere l'esposizione del proprio volto dinanzi alla fotocamera dell'apparecchio.

Non sono noti, con sufficiente grado di dettaglio, i rischi di *bias* con potenziali effetti discriminatori[59], del resto tardivamente venuti a emersione e, poi, specificamente accertati (e correlati, all'insegna del meccanismo *garbage in/garbage out*, a errori di implementazione e selezione dei dati introdotti nel *data base* posto a disposizione del *software*) in recenti esperienze straniere relative all'applicazione di sistemi predittivi di intelligenza artificiale, in particolare, in materia di stima del rischio di recidiva[60].

Senz'altro opportuno è rilevare come, tra le previsioni del Regolamento europeo sull'intelligenza artificiale di recente entrata in vigore, fi-

[58] Il riferimento è, in particolare, a quanto accaduto in occasione della finale di UEFA *Champions League* di Cardiff del 2017, in occasione della quale oltre duemila persone sono state erroneamente identificate quali possibili sospettati di condotte criminali da un applicativo di riconoscimento facciale. Sul punto, J. Della Torre, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1066.

[59] J. Della Torre, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1067; A. Najibi, *Racial Discrimination in Face Recognition Technology*, 24 ottobre 2020, consultabile *on line* all'indirizzo: https://projects.iq.harvard.edu/sciencepolicy/blog/racial-discrimination-face-recognition-technology.

[60] Il riferimento è, anche qui, alla vicenda relativa all'impiego dell'applicativo COMPASS, già in precedenza menzionato e in relazione al quale si è, in particolare, accertato che gli imputati neri avevano molte più probabilità degli imputati bianchi di essere erroneamente giudicati a più alto rischio di recidiva. Sul punto, v. Del Gatto, *La* governance *delle nuove tecnologie tra tentativi di regolazione e istanze di* self regulation. *Il caso del riconoscimento facciale*, cit., 48; nonché J. Larson - S. Mattu - L. Kirchner - J. Angwin, *How We Analyzed the COMPASS Recidivism Algorithm*, 23 maggio 2016, reperibile all'indirizzo: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. In materia di giustizia penale predittiva, di grande interesse gli approfondimenti operati da B. Galgani, *Considerazioni sui "precedenti" dell'imputato e del giudice al cospetto dell'IA nel processo penale*, in *Sistema Penale*, 2020, 4, 81 ss.; e da S. Quattrocolo, *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in *Cass. Pen.*, 2019, 1748 ss.; in argomento v., altresì, V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in *disCrimen*, 15.5.2020, 9 ss.

guri una nutrita serie di disposizioni volte a imporre ai produttori e ai fornitori di tali tecnologie specifici obblighi di trasparenza e informazione rispetto alle concrete modalità di funzionamento, alle garanzie di sicurezza e all'affidabilità di tali strumenti[61], nonché di cooperazione con le autorità pubbliche che dovessero farvi ricorso[62].

Si tratta di previsioni, senz'altro apprezzabili, che perseguono l'ambizioso obiettivo di ridurre sensibilmente il tasso di «opacità» di cui tali applicativi appaiono contraddistinti ma la cui concreta idoneità a rimuovere i dubbi in ordine al loro legittimo impiego processuale è ancora tutta da verificare e, anzi, fortemente opinabile.

Ne consegue un quadro dello stato dell'arte piuttosto magmatico e, comunque, difficilmente suscettibile, quantomeno allo stato, di soddisfare il requisito dell'idoneità epistemologica previsto dall'art. 189 c.p.p. quale *conditio sine qua non* per consentire l'accesso dei sistemi di riconoscimento facciale nel giudizio penale[63].

6. *La contrarietà ai diritti fondamentali della persona dell'impiego delle tecnologie di riconoscimento facciale in ambito penale*

Un secondo ostacolo pone in discussione l'ammissibilità probatoria delle tecnologie in discussione.

Esso dipende dalla contrarietà del trattamento dei dati biometrici di cui esse si servono alle norme nazionali e sovranazionali poste a presidio del diritto alla riservatezza, della protezione dei dati personali e degli altri diritti fondamentali a essi strettamente correlati[64].

[61] V. *infra, sub* 9.

[62] V. *infra, sub* 9.

[63] In tal senso, A. Marandola, *Il riconoscimento facciale*, cit., 512; J. Della Torre, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1062; M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. proc.*, 2021, 1053; E. Sacchetto, Face to face: *il complesso rapporto tra* automated facial recognition technology *e processo penale*, in *La legislazione penale*, 16.10.2020, 14.

[64] In tal senso si è unanimemente espressa la dottrina. Tra molti, v. A. Marandola, *Il riconoscimento facciale*, cit., 509 ss., secondo la quale l'attività svolta dai moderni applicativi di riconoscimento facciale comporta la compromissione di diritti fondamentali, *in primis* quello alla riservatezza e alla protezione dei dati biometrici, alla cui protezione concorrono gli artt. 7 e 8 della cd. Carta di Nizza, nonché le disposizioni della CEDU, la quale, pur non prevedendo espressamente il diritto alla protezione dei dati, «considera la tutela degli stessi come necessariamente caratterizzante, ma distinta, rispetto alla garanzia del diritto al rispetto della vita privata e familiare, dunque, anche in base all'art. 52, par.

È indubbio che le informazioni e i dati desumibili dall'immagine del volto di una persona, in quanto «dati biometrici intesi a identificare in modo univoco una persona fisica», siano incluse nel novero delle «categorie particolari di dati personali», di cui l'art. 9 comma 1 del Reg. 2016/679UE vieta il trattamento, salvo il caso in cui, ai sensi del comma 2 lett. g) della medesima disposizione, questo si renda necessario «per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

Tale previsione pare trovare un diretto contrafforte nell'art. 7 D.lgs. 51/2018 (attuativo della Dir. 2016/680UE), secondo il quale «il trattamento di dati di cui all'articolo 9 del regolamento UE è autorizzato solo se strettamente necessario e assistito da garanzie adeguate per i diritti e le libertà dell'interessato e specificamente previsto dal diritto dell'Unione

3, della CDFUE, risulta possibile operare dei riferimenti incrociati tra la giurisprudenza della CGUE e quella della Corte EDU». La stessa A. rileva come «la matrice ideale è quella del rifiuto di intrusioni in una sfera riconosciuta come propria della persona e della sua spontanea socialità […] che trova fondamento nell'art. 2 Cost., in quanto collocata nella dimensione delle relazioni sociali e del pieno svolgimento della propria personalità, e nell'art. 3 Cost., ove si menziona l'eguaglianza e la "dignità sociale"». Diritti che, peraltro, «si legano ad altre previsioni costituzionali, in relazione ai profili specifici, a partire dall'art. 13 Cost. alla libertà personale intesa come comprendente l'integrità psichica e coscienziale, nonché la tutela del domicilio (art. 14 Cost.), delle comunicazioni (art. 15) e della manifestazione del pensiero (art. 21 Cost.)». In senso adesivo, J. Della Torre, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1068 ss., il quale sottolinea come tali tecnologie «impattino, allo stesso tempo, sia sul diritto all'"identità personale", sia sul cosiddetto *habeas data* – da intendersi come prerogativa dell'individuo di mantenere il controllo sulle informazioni concernenti il proprio corpo virtuale e di opporsi alle interferenze altrui sulle stesse – elaborato dalla migliore dottrina, in chiave evolutiva, dal canone tradizionale dell'*habeas corpus*». Al riguardo, non va, peraltro, trascurato almeno un riferimento alla possibilità che l'estensivo impiego di tali strumenti tecnologici possa ingenerare il cd. *chilling effect*, concetto elaborato dalla dottrina che paventa il rischio che l'individuo, per il timore o la consapevolezza di essere sorvegliato, possa spontaneamente rinunciare alla fruizione di diritti a esercizio collettivo. In tal senso, tra molti, S. Del Gatto, *La* governance *delle nuove tecnologie*, cit., 47. Per un'ampia panoramica in materia, v. G. Mobilio, *Tecnologie di riconoscimento facciale*, cit., 57 ss.; M. Colacurci, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini,* in *Sistema Penale*, 2022, 23 ss.; E. Currao, *Il riconoscimento facciale e i diritti fondamentali: quale equilibrio?*, in *Diritto Penale e Uomo*, 2021, 1 ss.; F. De Simone, *Una nuova tipologia di misure di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale*, in *Arch. Penale*, 2023, 2, 18 ss.

europea o da legge o, nei casi previsti dalla legge, da regolamento, ovvero, ferme le garanzie dei diritti e delle libertà, se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica o se ha ad oggetto dati resi manifestamente pubblici dall'interessato».

Si tratta di disposizioni che, com'è noto, si limitano a dettagliare e specificare il contenuto di diritti della persona già riconosciuti e presidiati da un ampio novero di disposizioni di rango costituzionale e convenzionale, poste a salvaguardia delle libertà fondamentali, tra le quali giova richiamare gli artt. 2, 3, 13 e 117 Cost., gli artt. 7 e 8 della Carta di Nizza, l'art. 8 della Convenzione EDU[65].

La composita trama normativa sopra richiamata condiziona, dunque, la legittimità del trattamento di tali dati sensibili, in assenza del consenso della persona interessata, a un duplice ordine di requisiti: l'esistenza di una base normativa sufficientemente dettagliata; la conformità della disciplina legislativa *de qua* al principio di proporzionalità di matrice euro unitaria.

Ne discende, che, *de iure condito*, in carenza del consenso della persona interessata, l'impiego immagini facciali, all'interno di un sistema di *facial recognition* debba considerarsi alla stregua di un illecito trattamento di dati biometrici, per giunta lesivo di un vasto novero di diritti fondamentali oggetto di specifica previsione sia costituzionale sia ad opera delle più importanti Carte internazionali poste a protezione dei diritti individuali[66].

A tal riguardo è, tuttavia, opportuno precisare come l'Autorità Garante per la Protezione dei Dati Personali abbia offerto, sul punto, delle indicazioni parzialmente contraddittorie.

Nel parere, reso nell'anno 2018, sull'applicativo SARI *Enterprise*, si è infatti espresso un giudizio favorevole all'impiego di tale tecnologia, richiamando, a conforto di tale conclusione: da un lato, la legittimità della acquisizione dei dati biometrici immessi nella piattaforma denominata AFIS, costituente il *database* attraverso il quale opera il suddetto *software*; dall'altro, la possibilità di individuare (tra le altre disposizioni citate, di rilievo *extra* penale) nel dettato dell'artt. 349 c.p.p. una base normativa adeguata a soddisfare i requisiti di liceità del trattamento, al lume delle disposizioni interne e sovranazionali.

[65] Sul punto cfr. nota precedente.

[66] Marandola, *Il riconoscimento facciale*, cit., 514; J. Della Torre, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1082; M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. proc.*, 2021, 1052.

Di segno opposto è stato, invece, il parere, reso nel 2021, relativo all'impiego dell'applicativo SARI *Real Time*, sul presupposto che l'acquisizione e l'elaborazione dei dati biometrici vagliati dal suddetto *software* esporrebbe una serie indeterminata di persone a un trattamento di dati non disciplinato dalla legge, né giustificato da ragioni idonee a soddisfare il principio di proporzionalità[67].

Ne consegue che, nonostante quanto sin qui osservato e quantomeno per ciò che concerne l'utilizzo di SARI *Enterprise* in ambito penale, la possibilità di predicarne la illiceità sia tutt'altro che scontata, trovando – anzi – nel suddetto parere la tesi che ne riconosce la piena legittimità autorevole conferma.

È, tuttavia, opportuno osservare – quantomeno per ciò che concerne il procedimento penale – come la base normativa rinvenuta dal Garante nell'art. 349 c.p.p., appaia, al più, legittimare il ricorso a tale strumento solo nel corso delle indagini preliminari e limitatamente allo scopo di procedere alla «identificazione della persona nei cui confronti vengono svolte le indagini e di altre persone» (argomento sul quale si tornerà più approfonditamente *infra sub* 8).

Sicché, impregiudicata la possibilità di ritenere tale richiamo normativo sufficiente ad autorizzare il trattamento di dati biometrici operato dall'applicativo SARI *Enterprise*, appare arduo sostenere che tale previsione possa offrire adeguata "copertura legislativa" rispetto all'applicazione di tale strumento anche nella fase del giudizio e, dunque, con finalità di prova, tenuto conto della marcata eterogeneità strutturale e funzionale delle due fasi già in precedenza illustrata.

7. *Prove atipiche e diritti fondamentali*

La contrarietà del trattamento di dati biometrici posto in essere dagli applicativi di *facial recognition* ai diritti fondamentali e alle previsioni di legge in precedenza annoverati induce ad affrontare il tema della loro ammissibilità, in guisa di prova non disciplinata dalla legge e, dunque, ai sensi dell'art. 189 c.p.p., anche sotto questo versante.

È ben noto che il tema della ammissibilità della prova cosiddetta incostituzionale, in quanto implicante una diretta violazione dei diritti fon-

[67] In argomento per una approfondita disamina dei provvedimenti del Garante, L. Saponaro, *Le nuove frontiere dell'individuazione personale*, in *Arch. Penale*, 2022, 1 ss.

damentali della persona, non abbia ancora trovato una stabilità nella lettura della dottrina e della giurisprudenza.

Compiendo uno sforzo di massima sintesi, indubbiamente riduttivo della estrema complessità della questione e delle varie opinioni scientifiche espresse in materia, può osservarsi come siano almeno tre le diverse ipotesi ricostruttive "sul campo".

La prima postula la possibilità di desumere direttamente dalla Costituzione la regola di esclusione probatoria che legittimerebbe, ai sensi dell'art. 191 c.p.p., l'identificazione di un divieto di ammissione e di acquisizione della prova suscettiva di violare un diritto fondamentale, sulla falsariga delle esperienze degli ordinamenti processuali di *common law*.

Tale teoria, che si potrebbe definire come implicante una forma di "tutela diretta" del diritto di rango costituzionale inciso, ha trovato eco in almeno due autorevoli precedenti.

Il primo di essi è da ravvisarsi nella sentenza della Corte costituzionale n. 34 del 1973, pronunciata in un'epoca in cui la categoria dell'inutilizzabilità non era ancora stata introdotta nel codice di rito.

In questa occasione, il Giudice delle leggi, chiamato a indagare i rapporti tra diritto al silenzio e attività di intercettazione di comunicazioni, aveva, infatti, espressamente osservato che «attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito»[68].

Deve riconoscersi, però, a tale affermazione la natura di mero *obiter dictum*, non essendo a tale rilievo seguita una decisione di illegittimità costituzionale[69].

Analogo discorso vale per la prima parte della motivazione della sentenza delle Sezioni unite della Suprema Corte di Cassazione n. 3 del

[68] Corte cost., 6 aprile 1973, n. 34 in *Giur. cost.*, 1973, 331 ss., con nota di V. Grevi, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche*. Per un'articolata esposizione della teoria della prova incostituzionale, senza pretesa di esaustività, oltre alla nota già menzionata, P. Nuvolone, *Le prove vietate nel processo penale nei paesi di diritto latino*, in *Riv. dir. proc.*, 1966, 442 ss.; F. Caprioli, *Colloqui riservati e prova penale*, Giappichelli, 2000, 236 ss.; F. M. Grifantini, *Il segreto difensivo nel processo penale*, Giappichelli, 2001, 279 ss.; A. Camon, *Le riprese visive come mezzo d'indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen.*, 1999, 1196 ss.; G. Spangher, *«E pur si muove» dal* male captum bene retentum *alle* esclusionary rules, in *Giur. cost.*, 2001, 2829 ss.; L. P. Comoglio, *Perquisizione illegittima ed inutilizzabilità derivata delle prove acquisite con il susseguente sequestro*, in *Cass. pen.*, 1996, 1548 ss.

[69] F. Cordero, *Procedura penale*, IX ed., Giuffrè, 2012, 641.

1996[70], in materia di rapporti tra perquisizione illegittima e sequestro, nella quale la tesi della "prova incostituzionale" sembra trovare una sponda.

Si tratta, tuttavia, di una decisione – icasticamente definita come «testo *à double face*»[71] – che è giunta a esiti decisori del tutto contraddittori con l'astratta evocazione di principio contenuta nella prima parte dell'esposizione motivazionale, giungendo a ribadire il tradizionale principio *male captum bene retentum*, a significare la natura esclusivamente processuale dei divieti probatori e, dunque, a sbarrare la strada all'ingresso nell'ordinamento della cd. inutilizzabilità derivata, di ascendenza anglosassone (dov'è meglio nota come *fruits of poisonous tree doctrine*)[72].

Si è, infatti, conclusivamente stabilita l'insussistenza di un rapporto di consequenzialità, giuridicamente rilevante, tra perquisizione illegittima e sequestro e, per l'effetto, riconosciuta la piena utilizzabilità dei beni sottoposti al vincolo di indisponibilità del sequestro probatorio, quand'anche materialmente rinvenuti all'esito di un'attività di ricerca della prova illegittima o, addirittura, integrante una condotta illecita sul piano del diritto sostanziale[73].

Un secondo approccio al tema della cd. "prova incostituzionale" è

[70] Cass., Sez. un., 27 marzo 1996, n. 5021, Sala, in *Cass. pen.*, 1996, 3268 ss., con osservazioni di M. Vessichelli.

[71] F. Cordero, *Procedura penale*, cit., p. 647.

[72] "Sbarramento" che, del resto, appare essere stato recepito come tale ed esplicitamente asseverato non solo dalla successiva giurisprudenza di legittimità ma, altresì, da una recente decisione della Corte costituzionale, nella quale si dà atto espressamente che «è soltanto la legge a stabilire quali siano – e come si atteggino – i divieti probatori» e, per l'effetto, si sottolinea come sia «lo stesso sistema normativo ad avallare la conclusione secondo la quale, per la inutilizzabilità che scaturisce dalla violazione di un divieto probatorio, non possa trovare applicazione un principio di "inutilizzabilità derivata", sulla falsariga di quanto è previsto, invece, nel campo delle nullità, dall'art. 185, comma 1, c.p.p.». Nella stessa decisione si è, inoltre, utilmente chiarito come la possibilità di accedere a una diversa ricostruzione degli effetti della sanzione di inutilizzabilità sugli atti, asseritamente, susseguenti a quello vietato dalla disciplina processuale rappresenti una opzione di politica legislativa di esclusivo appannaggio del legislatore (dunque, non suscettibile di essere introdotta attraverso una decisione "manipolativa" del Giudice delle leggi), anche in considerazione della natura eminentemente profilattica delle *esclusionary rules* che, invece, nei principali ordinamenti processuali di *common law*, hanno legittimato l'elaborazione e il recepimento della cd. "teoria dei frutti dell'albero avvelenato". Sul punto, v. Corte cost., 3 ottobre 2019, n. 219, in *Dir. pen. proc.*, 2020, 51 ss.

[73] A sostegno della tesi secondo la quale le prove acquisite in violazione di leggi penali sostanziali, ancorché risultanti in una lesione dei diritti fondamentali della persona, sarebbero da ritenersi utilizzabili, senza pretesa di esaustività, F. Cordero, *Procedura pe-*

rappresentato dall'opinione di quanti negano la possibilità di desumere, in via interpretativa, dalla previsione costituzionale di un diritto fondamentale un divieto processuale di ammettere e, dunque, acquisire la prova, sul presupposto che gli unici divieti probatori cui si riferisce l'art. 191 c.p.p. siano da ricavarsi dalla legge processuale[74].

Ciò con la conseguenza che l'esistenza di una norma processuale astrattamente suscettiva di legittimare l'ammissione e l'assunzione di una prova non conforme ai dettami della Costituzione e, persino, illecita, dovrebbe condurre il giudice chiamato ad applicarla ad attivare la procedura inciden-

nale, cit., 646 ss.; F. Caprioli, *Colloqui riservati*, cit., 232 ss.; N. Galantini, voce *Inutilizzabilità*, in *Enc. dir.*, Agg. I, Giuffrè, 1997, 700; Id., *L'inutilizzabilità della prova nel processo penale*, Cedam, 1992, 213 ss.; G. Illuminati, *L'inutilizzabilità della prova nel processo penale italiano*, in *Riv. it. dir. proc. pen*., 2010, 534 ss.; *contra*, per tutti, M. Nobili, sub *art. 191,* in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, II, Utet, 1990, 412 ss.; P. Nuvolone, *Le prove vietate nel processo penale*, cit., 474; S. Marcolini, *Regole di esclusione e nuove tecnologie*, in *Criminalia*, 2006, 1, 419. In argomento, v., altresì, C. Conti, *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, 2007; F.M. Grifantini, voce *Inutilizzabilità*, in *Dig. disc. pen*., VII, Utet, 1993, 242 ss.; E. N. La Rocca, voce *Inutilizzabilità*, in *Dig. disc. pen*., Agg. I, Utet, 2008, 613 ss.; Id., voce *Regola di esclusione*, in *Dig. disc. pen*., Utet, 2016, 620 ss; A. Scella, *L'inutilizzabilità della prova nel sistema del processo penale*, in *Riv. it. dir. proc. pen*., 1992, 203 ss.; Id., *Prove penali e inutilizzabilità. Uno studio introduttivo*, Giappichelli, 2000.

[74] Capofila di tale orientamento, poi sostenuto e ribadito dalla dottrina orientata a disconoscere che l'inutilizzabilità delle prova possa discendere dalla violazione di una disposizione sostanziale (cfr. nota precedente), è senz'altro F. Cordero, *Prove illecite nel processo penale*, in *Jus*, 1961, 73 ss. poi confluito in Id., *Il procedimento probatorio*, in *Tre studi sulle prove penali*, Giuffrè, 1963, secondo il quale «i precetti costituzionali rappresentano altrettanti paradigmi della normazione attuata in sede legislativa; ma s'incorre in un salto logico, quando si postula che la reazione dell'ordinamento giunga al punto di rifiutare, come processualmente irrilevante, ogni dato conoscitivo conseguito con una condotta difforme da quelle direttive […] se tali prove siano o meno ammissibili, è quesito che esige di essere risolto in base ad un'interpretazione sistematica delle norme processuali, salvo poi verificare se la disciplina di cui si è ricostruito l'assetto, non confligga con i principi della Costituzione» (pag. 154). Osservazione che, con ogni evidenza, vale a escludere la possibilità di giudicare inammissibili e, dunque, se già assunte, inutilizzabili prove la cui acquisizione si risolva nella violazione di un diritto tutelato dalla Costituzione ma non equivale a escludere che al suo interno possano rinvenirsi specifici divieti di acquisizione della prova, ben potendo la Costituzione contenere anche norme a carattere processuale: «Le valutazioni d'ammissibilità, notavamo, discendono da norme processuali: nelle procedure codificate le contengono gli articoli sulle prove, ma forse ne vigono d'extravaganti (ad esempio, immunità diplomatiche, quando implichino limiti al potere istruttorio); non esistono limiti alla topografia delle possibili fonti, purché siano norme situate a livello "legge"; e nessuna impossibilità teorica esclude norme processuali nella Costituzione». Così F. Cordero, *Procedura penale*, cit., 639.

tale finalizzata a consentire il vaglio del Giudice delle leggi e, nel caso, schiudere il varco a una declaratoria di illegittimità della suddetta previsione.

Una simile prospettazione, chiaramente conducente a configurare una forma di "tutela indiretta" del diritto fondamentale vulnerato, ha trovato anch'essa autorevole conferma nella giurisprudenza costituzionale, ben rappresentata dalla decisione della Consulta n. 238 del 1996, esitata nella declaratoria di illegittimità dell'art. 224 comma 2 c.p.p. «nella parte in cui consente che il giudice, nell'ambito delle operazioni peritali, disponga misure che comunque incidano sulla libertà personale dell'indagato o dell'imputato o di terzi, al di fuori di quelle specificamente previste nei "casi" e nei "modi" dalla legge»[75].

In posizione mediana tra quelle appena sunteggiate, si pone quella che si potrebbe definire alla stregua di una sorta di variante della teoria della "tutela indiretta".

Si è infatti sostenuto che, ferma la validità di quest'ultima impostazione, essa possa subire un adattamento, implicante la necessità dell'interprete di scongiurare la declaratoria di incostituzionalità della norma processuale legittimante l'ammissione e acquisizione della prova incostituzionale attraverso un'operazione esegetica volta a desumere analogicamente dalla Carta fondamentale o dalle regole processuali disciplinanti fattispecie contigue una trama di garanzie minime idonee ad appianare i profili di possibile incostituzionalità[76].

Un simile approccio, che si potrebbe sinteticamente denominare come "teoria delle garanzie minime", può rinvenirsi nella sentenza della Corte costituzionale n. 81 del 1993[77] in materia di garanzie da osservarsi in sede di acquisizione dei cd. "dati esterni" del traffico telefonico, nel qual caso la declaratoria di illegittimità costituzionale fu scongiurata desumendo direttamente dall'art. 15 Cost. la necessità di procedere a simili acquisizioni previo provvedimento motivato dell'autorità giudiziaria.

La variabilità di posizioni, sin qui sunteggiata e tutt'ora esistente in dottrina e giurisprudenza, e l'estrema complessità della materia non impedisce, tuttavia, di inquadrare con sicurezza il tema dell'ammissibilità dei sistemi di riconoscimento facciale in rapporto ai profili di contrasto che essi presentano rispetto ai diritti fondamentali dei soggetti titolari dei dati biometrici da essi utilizzati.

[75] Corte cost., 9 luglio 1996, n. 238, in *Giur. cost.*, 1996, 3567 ss.

[76] Un simile approccio pare sostenuto da D. Zignani, *Una discutibile pronuncia in tema di prove illegittimamente carpite nel domicilio*, in *Cass. pen.*, 2004, 1316.

[77] Corte cost., 11 marzo 1993, n. 81, in *Giur. cost.*, 1993, 731 ss.

L'inquadramento di tali tecnologie nell'ambito delle prove non disciplinate dalla legge consente, infatti, di aggirare lo spinoso problema dogmatico e sistematico cui si è dianzi solo accennato, facendo diretto riferimento all'originale elaborazione concettuale operata dalle Sezioni unite della Suprema Corte nella sentenza n. 26795 del 2006, nel caso Prisco[78], che, ancor oggi, costituisce il *leading case* in materia di prove atipiche consistenti nello svolgimento di attività *contra legem* o, addirittura, suscettive di vulnerare un diritto fondamentale presidiato dalla Costituzione.

In tale occasione, il Massimo Collegio ha espressamente osservato come la soluzione di tale problema non richieda di prendere posizione sulla controversia in ordine alla prova incostituzionale ma possa essere diversamente risolta[79].

Nonostante tale manifestazione di intenti, è lecito osservare come la decisione della Corte – quantomeno in relazione al regime giuridico delle videoriprese di comportamenti non comunicativi in luoghi diversi dal domicilio ma investiti da una ragionevole aspettativa di *privacy* – abbia, in buona misura, implicitamente ricalcato lo schema concettuale della summenzionata "teoria delle garanzie minime", desumendo in termini analogici, per questo tipo di atti intrusivi, la necessaria applicazione della garanzia costituita dall'atto motivato dell'autorità giudiziaria.

Ciò che conta, ai fini che qui competono, è però richiamare la parte dell'esposizione motivazionale della sentenza citata nella quale, preso atto che la prova atipica è ontologicamente non disciplinata dalla legge, si osserva che, a differenza di quella tipica, essa non possa configurarsi quale attività in astratto sempre ammissibile, fatta salva l'individuazione di specifici divieti normativi[80].

[78] Cass., Sez. un., 28 marzo 2006, n. 26795, Prisco, in *Cass. pen.*, 2006, 4344, con nota di M. L. Di Bitonto, *Le riprese video domiciliari al vaglio delle Sezioni unite.*

[79] Cass., Sez. un., 28 marzo 2006, n. 26795, Prisco, cit.: «per giungere alla conclusione che non possono considerarsi ammissibili, come prove atipiche, le videoregistrazioni di comportamenti non comunicativi effettuati in ambito domiciliare non occorre però prendere posizione sul dibattito relativo agli effetti che la violazione delle norme costituzionali di garanzia può avere sull'attività probatoria prevista dal codice di rito, né stabilire se la sanzione dell'inutilizzabilità attenga solo alla violazione dei divieti stabiliti dalla legge processuale o riguardi anche la violazione di norme costituzionali o di altri rami dell'ordinamento, e segnatamente di quello penale (come per le intrusioni nell'ambito domiciliare potrebbe prospettarsi con riferimento all'art. 615 bis c.p.). A ben vedere nel caso in esame questi aspetti controversi non vengono in questione perché la soluzione passa direttamente attraverso l'interpretazione dell'art. 189 c.p.p., che è stato richiamato per legittimare processualmente l'attività probatoria "incostituzionale"»

[80] Cass., Sez. un., 28 marzo 2006, n. 26795, Prisco, cit.: «si vuole dire che il tema

A tale rilievo consegue la necessità di investire il giudice dibattimentale di una valutazione preliminare di ammissibilità della prova innominata necessariamente più ampia e del tutto originale rispetto a quella attivata dalla richiesta di assumere una prova prevista dalla legge processuale. Valutazione che, in particolare, postula ed esige la scrupolosa verifica che l'attività euristica in cui essa consiste non si ponga in contrasto né con le regole processuali né con il diritto sostanziale, sia esso di fonte primaria o addirittura costituzionale, sul presupposto secondo il quale «non può considerarsi "non disciplinata dalla legge" una prova basata su un'attività che la legge vieta»[81].

Com'è stato precisamente osservato, è del resto perfettamente ragionevole sostenere che «il divieto legale cui fare riferimento per legittimare l'esclusione della prova da parte del giudice non possa non avere differente fonte normativa a seconda che la prova sia tipica o no. Solo nel primo caso, infatti, il divieto è rinvenibile nel codice di procedura penale; rispetto alle prove atipiche, invece, bisognerà avere riguardo agli eventuali divieti stabiliti in altre parti dell'ordinamento»[82].

Tale elaborazione concettuale è gravida di implicazioni nel caso dei sistemi di riconoscimento facciale e costituisce una guida sicura per risolvere il tema oggetto di analisi.

Essa consente, in particolare, di addivenire alla conclusione che, laddove tali tecnologie si ritenessero integranti un illecito trattamento di dati biometrici e, dunque, suscettive di vulnerare il diritto alla riservatezza e alla protezione dei dati personali delle persone coinvolte, non potrebbero conseguentemente dirsi ammissibili, quali prove innominate, ai sensi dell'art. 189 c.p.p.

In difetto di un'articolata e calibrata disciplina legislativa, non pare

della inutilizzabilità come sanzione processuale per la violazione di regole di rango costituzionale riguarda, in linea di principio, le prove tipiche e non quelle atipiche. Prima dell'ammissione le prove atipiche non sono prove, perciò se sorge questione sulla legittimità delle attività compiute per acquisire i materiali probatori che le sorreggono ci si deve interrogare innanzi tutto sulla loro ammissibilità, piuttosto che sulla loro utilizzabilità, e a parere di queste Sezioni unite se si fa corretta applicazione dell'art. 189 c.p.p. le videoregistrazioni acquisite in violazione dell'art. 14 Cost. devono considerarsi inammissibili. Infatti l'art. 189 c.p.p., in coerenza con l'art. 190 c.p.p., comma 1, – che impone al giudice di escludere le prove "vietate dalla legge" –, presuppone logicamente la formazione lecita della prova e soltanto in questo caso la rende ammissibile. Il presupposto è implicito, dato che per il legislatore non poteva che essere lecita un'attività probatoria "non disciplinata dalla legge"».

[81] Cass., Sez. un., 28 marzo 2006, n. 26795, Prisco, cit.

[82] M. L. Di Bitonto, *Le riprese video domiciliari al vaglio delle Sezioni unite,* cit., 3960.

allora azzardato rintracciare nell'illiceità del trattamento dei dati svolto da tali applicativi nella contrarietà del loro impiego ai diritti fondamentali della persona un ulteriore e invalicabile ostacolo all'ammissione degli strumenti di *facial recognition* nel sistema delle prove penali[83].

8. *Tecnologie di riconoscimento facciale in ambito investigativo*

Come già accennato, la fase delle indagini preliminari si conforma a una "logica" eterogenea rispetto a quella propria del giudizio, in quanto contraddistinta da una tendenziale atipicità.

Rilevata "l'apertura" di questo segmento del procedimento penale all'espletamento di attività non disciplinate dalla legge, occorre domandarsi se le tecnologie di riconoscimento facciale possano costituire un legittimo strumento di investigazione.

Per rispondere al quesito occorre prioritariamente rilevare come sussista una certa diversificazione di posizioni tra la dottrina e la giurisprudenza in materia.

Secondo l'opinione della migliore dottrina, l'attività di investigazione atipica non sarebbe disciplinata ai sensi dell'art. 189 c.p.p., nonostante – in linea di principio – i principi sulle prove debbano essere estesi anche alla fase preliminare[84].

Lo svolgimento di atti atipici di indagine, specie se consistenti nel compimento di atti intrusivi della riservatezza posti in essere attraverso il ricorso a nuove tecnologie, infatti, difficilmente si concilierebbe con il vaglio preliminare di ammissibilità – da esperirsi in contraddittorio e da intendersi finalizzato anche a definire le specifiche modalità acquisitive della prova[85] – che la disposizione da ultimo citata demanda al giudice richiesto di assumere una prova non disciplinata dalla legge; né potrebbe individuarsi nell'art. 189 c.p.p., previsione caratterizzata da intrinseca va-

[83] In tal senso, sia pure con differenti sfaccettature, A. Marandola, *Il riconoscimento facciale*, cit., 511; J. Della Torre, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1081; M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, cit., 64.

[84] Per tutti, A. Camon, *Le indagini preliminari*, cit., 474.

[85] In tal senso, altresì, O. Mazza, *I diritti fondamentali dell'individuo come limite della prova,* cit., 9, secondo il quale «l'art. 189 c.p.p. parla, non a caso, di modalità assuntive che devono essere determinate dal giudice, il che lascia chiaramente intendere come la finestra delle prove atipiche si affacci solo sul cortile del dibattimento per accogliere i mezzi di prova costituenda innominati».

ghezza, una norma idonea a disciplinare l'amplissima varietà di situazioni e atti suscettivi di essere espletati nella fase investigativa[86].

Si tratta di un assunto certamente condivisibile, a conforto del quale dovrebbe aggiungersi la semplice quanto persuasiva argomentazione secondo cui, come già rilevato, tale previsione – dettata per il dibattimento – si colloca in un rapporto di regola a eccezione rispetto al principio di legalità della prova e, dunque, di tendenziale tassatività dei mezzi istruttori sagomati nel libro terzo del codice di rito.

Dal punto di vista sistematico è, dunque, possibile ritenere l'art. 189 c.p.p. alla stregua di una norma speciale, orientata a consentire limitate deroghe a questo principio in seno alla fase del giudizio.

Ne consegue, a stretto rigore, che di essa non possa farsi interpretazione analogica e, dunque, che non possa valere a disciplinare l'attività di investigazione atipica che trova collocazione nella fase delle indagini preliminari, diversamente da quanto accade per le regole generali del diritto delle prove penali.

Le ricadute logiche di una simile prospettazione conducono a ritenere le attività atipiche di indagine consentite nel limite del rispetto dei diritti fondamentali delle persone coinvolte e delle norme di diritto sostanziale generalmente applicabili.

La giurisprudenza propende, invece, per l'applicazione analogica dell'art. 189 c.p.p. alla fase preliminare, sia pure – come chiarito dalle solite Sezioni unite Prisco – «con gli opportuni adattamenti», essenzialmente consistenti nella posticipazione alla fase del dibattimento dell'instaurazione del contradditorio in ordine alla ammissibilità del risultato di conoscenza acquisito attraverso l'attività di investigazione atipica.

Tenuto conto di quanto già esposto nel precedente paragrafo e della specificità della questione oggetto di analisi, non è, tuttavia, necessario soffermarsi ulteriormente su tale controversia, potendosi concludere che, tanto nel primo, quanto nel secondo caso, la legittimità dell'impiego di sistemi di *facial recognition* in ambito investigativo incontrerebbe l'identico ostacolo, costituito dalla sua contrarietà alle norme disciplinanti il trattamento di dati biometrici e ai diritti fondamentali di cui esse sono espressione.

Se, dunque, l'espletamento di tali attività dovesse effettivamente ritenersi connotata dai profili di illiceità in precedenza segnalati, dovrebbe

[86] Per tutti, A. Camon, *Le indagini preliminari*, cit., 474 ss.

conseguentemente ritenersi precluso, in ogni caso, il ricorso alle predette tecnologie, anche nella fase investigativa.

Ciò detto, occorre, però, ancora confrontarsi col il parere favorevole reso dal Garante Nazionale per la Protezione dei Dati Personali rispetto all'impiego di SARI *Enterprise* in ambito investigativo, che ha individuato – per ciò che concerne la disciplina processuale – nell'art. 349 c.p.p. un'adeguata base normativa legittimante il trattamento di dati biometrici dei soggetti coinvolti; e con il dato, restituito dall'esperienza giudiziaria, che in diversi procedimenti in corso sia stato certamente fatto ricorso a tale applicativo al fine di individuare possibili sospettati.

È infatti agevole prevedere che se l'opinione della suddetta Autorità amministrativa dovesse essere condivisa dalla giurisprudenza – allo stato silente – tanto legittimerebbe un estensivo ricorso a tale strumento nell'ambito delle investigazioni penali.

Impregiudicati i dubbi, in punto di diritto sostanziale, che l'opinione espressa dal Garante autorizza, non pare azzardato osservare come l'individuazione dell'art. 349 c.p.p. quale norma idonea a legittimare il ricorso alle tecnologie di riconoscimento facciale presti il fianco a serie perplessità di ordine schiettamente processuale.

Se è vero che la disposizione richiamata stabilisce che «la polizia giudiziaria procede alla identificazione della persona nei cui confronti vengono svolte le indagini e delle persone in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti» e che tanto possa avvenire anche eseguendo, «ove occorra, rilievi dattiloscopici, fotografici e antropometrici nonché altri accertamenti»; non è men vero che tale previsione sembri limitarsi a disciplinare un'attività – quella, appunto, tesa alla «identificazione» – che poco o nulla ha a che vedere con quella che il ricorso alle tecnologie di cui si discute promette di agevolare.

È lecito ritenere che, nel fuoco dell'art. 349 c.p.p. e nel contesto delle norme disciplinate nel libro quarto del codice di rito, il concetto di «identificazione» debba intendersi riferito all'attribuzione di generalità anagrafiche a chi ne sia privo o alla loro verifica nei casi in cui queste possano ritenersi dubbie[87].

La ricerca del sospettato o delle persone informate sui fatti non trova, infatti, collocazione all'interno di questa disposizione, bensì negli artt. 55, 348 e 361 c.p.p. (le prime due destinate a disciplinare le attività della polizia giudiziaria, l'ultima concernente il pubblico ministero), nessuna

[87] M. L. Di Bitonto, *I soggetti*, in A. Camon, M. Daniele, D. Negri, C. Cesari, M. L. Di Bitonto, P. P. Paulesu, *Fondamenti di procedura penale,* cit., 220, che osserva: «L'in-

delle quali contiene un riferimento analogo a quello previsto dall'art. 349 comma 2 c.p.p. circa la possibilità di procedere ad «altri accertamenti» nel loro espletamento.

Non a caso, proprio l'art. 361 c.p.p., che costituisce – per opinione unanime – l'atto omologo della ricognizione personale[88], di cui all'art. 213 c.p.p., definisce tale attività investigativa utilizzando il diverso e molto più pertinente lemma di «individuazione di persone e cose», a significare che la ricerca e, appunto, "l'individuazione" della persona cui la notizia di reato è attribuita o di quelle in grado di riferire su di essa poco o nulla abbia a che vedere con l'attribuzione di generalità anagrafiche.

Ne consegue che l'estemporaneo riferimento all'ampia e indeterminata previsione dell'art. 349 c.p.p., operato dal Garante, non consente di ritenere né che l'impiego di tecnologie di riconoscimento facciale sia attività riconducibile a un atto tipico della polizia giudiziaria, né di concludere che tale disposizione normativa garantisca una adeguata "copertura normativa" al trattamento di dati biometrici con finalità investigativa.

9. *Le condizioni di liceità dell'impiego delle tecnologie di riconoscimento facciale alla luce del Regolamento europeo sull'intelligenza artificiale di recente introduzione*

Il Regolamento europeo n. 2024/1689/UE, di recente entrata in vigore ma sottoposto a una composita disciplina intertemporale[89], contiene un nutrito novero di previsioni destinate a regolamentare l'immissione in commercio e l'impiego delle tecnologie basate sull'intelligenza artificiale e, tra queste, dei moderni sistemi di riconoscimento facciale[90].

Per sua natura, tale atto normativo non disciplina la materia processuale.

dividuazione della persona sottoposta a procedimento penale è concetto distinto dalla sua identificazione e soltanto la prima è condizione essenziale per l'instaurazione del procedimento. Individuare una persona significa precisare quale sia l'uomo o la donna cui attribuire il fatto di reato e nei cui confronti svolgere le indagini e poi, eventualmente, esercitare l'azione penale. Identificare qualcuno, invece, significa attribuire un'identità alla persona individuata».

[88] A. Camon, *Le indagini preliminari*, in A. Camon, M. Daniele, D. Negri, C. Cesari, M. L. Di Bitonto, P. P. Paulesu, *Fondamenti di procedura penale*, cit., 468.

[89] V. retro, *sub* nota n. 11.

[90] In argomento, v. G. Canzio, AI Act *e processo penale: sfide e opportunità*, in *Sistema*

Esso, tuttavia, introduce un articolato novero di previsioni che valgono a sagomare le condizioni di liceità del ricorso a tali tecnologie sia nell'ambito dei rapporti privati sia in seno alle attività di rilievo pubblico.

Giova rimarcare subito che la nuova disciplina, in maniera espressa, fa salve le previsioni del diritto europeo in materia di protezione dei dati personali[91]. Di conseguenza, tutte le considerazioni prima svolte – relative alla discussa compatibilità del ricorso agli strumenti di riconoscimento facciale con le disposizioni, europee e nazionali, poste a salvaguardia della riservatezza e della protezione dei dati biometrici – non sono in alcun modo da aggiornare alla luce della nuova disciplina. Anzi, come sarà più chiaro nel prosieguo della disamina, vengono introdotti requisiti per l'impiego degli strumenti che consentono l'identificazione biometrica della persona ulteriori, rispetto a quelli già espressamente previsti o, comunque, deducibili dalla disciplina posta a salvaguardia dei diritti della persona in precedenza annoverati.

Dalla lettura del Regolamento si rileva come, a seconda delle loro caratteristiche tecniche, i sistemi di riconoscimento facciale possano ricadere, alternativamente, nell'ambito delle «pratiche vietate», di cui all'art. 5, ovvero nell'ambito dei «sistemi di IA ad alto rischio», di cui agli artt. 6 ss.

Nella prima categoria, ai sensi della lett. h) del paragrafo 1 dell'art. 5 suddetto, rientrano «i sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico», così dovendosi intendere gli applicativi che – sul modello di SARI *Real Time*, già bocciato dal Garante italiano – consentono l'identificazione automatizzata della persona, mediante la comparazione di dati biometrici, tra i quali le immagini facciali, in termini pressoché istantanei.

Il divieto posto dalla disciplina europea non è, tuttavia, assoluto.

La medesima disposizione sopra citata eccettua, infatti, dall'area delle pratiche vietate l'impiego di tali strumenti in presenza di due requisiti concorrenti.

Il primo è individuato nello svolgimento di una «attività di contrasto», concetto da inquadrarsi – ai sensi dell'art. 3 paragrafo 45 del suddetto Regolamento – nell'attività svolta dalle autorità pubbliche «a fini di prevenzione, indagine, accertamento o perseguimento di reato o di ese-

penale, 14 ottobre 2024; nonché C. Teresi, *L'*AI Act *nell'ottica del processual-penalista: uno sguardo preliminare*, in *Penale diritto e procedura*, 20 giugno 2024.

[91] V. art. 2, paragrafo 5, nonché art. 26, paragrafo 10.

cuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse».

Il secondo è da rinvenirsi nella assoluta necessità di ricorrere a tale pratica al fine di perseguire uno degli obiettivi specificamente indicati nel seguito della disposizione, vale a dire: «i) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; iii) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni».

Se inquadrate dal punto di vista del diritto processuale, si tratta di previsioni derogatorie sufficientemente ampie da legittimare il ricorso a simili strumenti in una vasta moltitudine di casi, quantomeno per finalità investigative o di ricerca della persona cui il reato è attribuito. Rilievo che induce a valorizzare ulteriormente i limiti al ricorso a simili tecnologie già in precedenza esaminati e deducibili dalle disposizioni interne.

In difetto dei presupposti sopra richiamati, il ricorso a sistemi di riconoscimento facciale in luoghi pubblici o aperti al pubblico "in tempo reale" deve, in ogni caso, considerarsi espressamente vietato dalla disciplina europea.

Al di fuori di tale ipotesi, l'impiego di strumenti di riconoscimento facciale, come detto, va inquadrata nel contesto delle previsioni destinate a disciplinare i «sistemi di IA ad alto rischio», di cui agli artt. 6 ss.

Tanto si deduce dall'espresso richiamo, operato dal paragrafo 2 della disposizione appena citata, ai sistemi di intelligenza artificiale menzionati nell'allegato III al Regolamento, tra i quali figurano «i sistemi di identificazione biometrica remota», con la sola (ma rilevante) eccezione dei «sistemi di IA destinati a essere utilizzati per la verifica biometrica la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere». Indicazione, quest'ultima, che pare rastremare il *genus* dei sistemi definiti ad alto rischio, eccettuando gli applicativi informatici sviluppati allo scopo esclusivo di verifica dell'identità dell'utente, al fine di consentire l'accesso a un sistema informatico protetto da *password* o ad accesso controllato.

Ne discende che i sistemi di *facial recognition* diversi da quelli operanti in modalità *real time* e per mezzo di videocamere posizionate in luoghi aperti al pubblico debbano – con buona approssimazione – considerarsi legittimi, sempre che siano osservate le prescrizioni di cui al capo III del Regolamento, destinate a disciplinare l'immissione in commercio e l'impiego dei sistemi di intelligenza artificiale ad alto rischio.

All'interno di questo ampio e articolato coacervo normativo si rinvengono, sostanzialmente, tre categorie di disposizioni: 1) quelle volte a disciplinare i requisiti tecnici e qualitativi di tali sistemi: 2) quelle finalizzate a stabilire i doveri dei fornitori e dei loro utilizzatori (nonché degli importatori e distributori); 3) quelle aventi a oggetto le modalità di esercizio dei poteri di controllo, registrazione e valutazione di conformità da parte degli enti pubblici preposti all'implementazione della disciplina europea.

Sorvolando su quest'ultima categoria, che non impatta direttamente sull'ambito processuale penale, può sinteticamente rilevarsi come il primo gruppo di norme (condensate nella Sezione 2 del Capo III) introduca un articolato ventaglio di disposizioni volte ad assicurare che i sistemi ad alto rischio presentino sufficienti garanzie di trasparenza, qualità, affidabilità e sicurezza[92]; nonché che siano progettati in maniera tale da garantire l'effettiva possibilità del controllo e della sorveglianza umani sul loro

[92] Tra queste, meritevoli di specifica menzione sono le previsioni di cui: all'art. 13, il quale – *inter alia* – prevede espressamente che le istruzioni per l'uso predisposte dai fornitori del sistema di IA contengano le informazioni sulle «caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, tra cui: i) la finalità prevista; ii) il livello di accuratezza che ci si può attendere, comprese le metriche, di robustezza e cibersicurezza di cui all'art. 15 rispetto al quale il sistema di IA ad alto rischio è stato sottoposto a prova e convalidato, e qualsiasi circostanza nota e prevedibile che possa avere un impatto sul livello atteso di accuratezza, robustezza e cibersicurezza; iii) qualsiasi circostanza nota o prevedibile connessa all'uso del sistema di IA ad alto rischio in conformità della sia finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile che possa comportare rischi per la salute e la sicurezza o per i diritti fondamentali di cui all'art. 9, paragrafo 2»; all'art. 15, il quale – *inter alia* – dispone che «i sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da conseguire un adeguato livello di accuratezza, robustezza e cibersicurezza e da operare in modo coerente con tali aspetti durante tutto il loto ciclo di vita», e prevede che «i sistemi di IA ad alto rischio che proseguono il loro apprendimento dopo essere stati immessi sul mercato o messi in servizio sono sviluppati in modo tale da eliminare o ridurre il più possibile il rischio di output potenzialmente distorti che influenzano gli input future (feedbacks loops - "circuiti di feedback") e garantire che tali circuiti di feedback siano oggetto di adeguate misure di attenuazione».

utilizzo[93]. In altre parole, tali disposizioni introducono una serie di requisiti volti a impedire l'immissione in commercio e il successivo utilizzo di *software* che non si conformino agli *standard* qualitativi, progettuali e di sicurezza appositamente previsti, stabilendo peraltro, nella successiva Sezione 3 del medesimo Capo, i conseguenti obblighi dei fornitori e degli utilizzatori di tali tecnologie (nonché dei loro importatori o distributori).

Se è piuttosto agevole rilevare che lo spettro dei doveri posti in capo ai fornitori implichi l'obbligo di garantire la sussistenza e la permanenza nel tempo degli *standard* qualitativi imposti dal Regolamento, è importante osservare come i predetti doveri si estendano a compiti di informazione e cooperazione con gli utilizzatori delle tecnologie di cui si discute, di documentazione e gestione dei dati da esse utilizzati, di conservazione dei dati relativi agli accessi alle banche dati o ai sistemi informatici suddetti[94].

Di particolare valore, inoltre, è quanto disposto dall'art. 26 paragrafo 10 del Regolamento, che disciplina gli obblighi degli utilizzatori dei sistemi di intelligenza artificiale ad alto rischio, tra i quali, nel caso di loro impiego nell'ambito del procedimento penale, devono senz'altro considerarsi ricomprese l'autorità giudiziaria e le forze di polizia giudiziaria[95].

[93] Rilevante, a tal proposito, è il dettato dell'art. 14, secondo il quale «i sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso», finalità rispetto alla quale decisiva è la previsione del successivo paragrafo 4, secondo la quale il fornitore è tenuto a porre l'utilizzatore nelle condizioni di «a) comprendere correttamente le capacità e i limiti pertinenti al sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese; b) restare consapevole della possibile tendenza a fare automaticamente affidamento o fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio ("distorsione dell'automazione), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche; c) interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili; d) decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio»

[94] Si veda, in particolare, l'art. 21, il quale stabilisce l'obbligo dei fornitori di tali tecnologie, su richiesta motivata di un'autorità competente, di fornire «tutte le informazioni e la documentazione necessarie per dimostrare la conformità del sistema di IA ad altro rischio ai requisiti di cui alla sezione 2», nonché di consentire l'accesso «ai log generati automaticamente del sistema di IA ad altro rischio».

[95] La norma si riferisce, infatti, espressamente ai doveri dei cosiddetti «deployer»,

La suddetta disposizione, oltre a fornire specifiche indicazioni circa la necessità di impiegare tali ritrovati in maniera conforme alle istruzioni d'uso e a sancire specifiche cautele tese a favorirne un impiego consapevole e informato, impone il rispetto di alcune garanzie procedurali minime, concernenti l'applicazione delle suddette tecnologie in ambito investigativo o processuale.

Allorché esse siano utilizzate per «la ricerca mirata di una persona sospettata o condannata per aver commesso un reato» si esige «un'autorizzazione, *ex ante* o senza indebito ritardo ed entro le 48 ore, da parte di un'autorità giudiziaria o amministrativa la cui decisione è vincolante e soggetta a controllo giurisdizionale, per l'uso di tale sistema, tranne quando è utilizzato per l'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato».

Si specifica, inoltre, che in tali casi «ogni uso è limitato a quanto strettamente necessario per le indagini su uno specifico reato» e che, se la suddetta autorizzazione è respinta, «l'uso del sistema di identificazione biometrica remota a posteriori collegato a tale autorizzazione richiesta è interrotto con effetto immediato e i dati personali connessi all'uso del sistema di IA ad alto rischio per il quale è stata richiesta l'autorizzazione sono cancellati».

Oltre a ciò, è pure introdotto uno specifico divieto delle suddette tecnologie «a fini di contrasto in modo non mirato, senza alcun collegamento con un reato, un procedimento penale, una minaccia reale e attuale o reale e prevedibile di un reato o la ricerca di una determinata persona scomparsa», con la ulteriore precisazione che «nessuna decisione che produca effetti giuridici negativi su una persona possa essere presa dalle autorità di contrasto unicamente sulla base dell'output di tali sistemi di identificazione biometrica remota a posteriori».

Si sancisce, in aggiunta, un generalizzato obbligo di documentazione, nel relativo fascicolo procedimentale o di polizia, del ricorso a tali strumenti tecnologici.

Con notazione di chiusura, si ribadisce, infine, la facoltà degli Stati membri di introdurre «misure più restrittive» che limitino il ricorso a si-

categoria che identifica, alla stregua della definizione fornita dall'art. 3 n. 4 dello stesso Regolamento, «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale». Si tratta, dunque, di definizione certamente comprensiva di qualsiasi autorità pubblica che, nello svolgimento dei propri compiti o funzioni, ricorra all'impiego di tali tecnologie.

mili applicativi, chiarendo ulteriormente la natura di *minimum standard* della disciplina contenuta nel Regolamento.

Degno di menzione, ancora, è il disposto del successivo art. 27, il quale demanda all'utilizzatore l'elaborazione di «una valutazione dell'impatto sui diritti fondamentali» che l'uso di tali strumenti può produrre, necessariamente comprensiva della disamina di una serie di elementi minuziosamente indicati.

Si tratta di un compendio molto ampio di prescrizioni che, come anticipato, concorrono a delineare una serie di condizioni di liceità dell'impiego, anche in ambito processuale, delle tecnologie basate sull'intelligenza artificiale, ivi incluse quelle finalizzate al riconoscimento facciale.

Tale complesso normativo rileva, per quanto qui compete, sotto duplice profilo.

Da un lato, rende urgente comprendere se la violazione dei requisiti e delle specifiche condizioni di impiego di simili tecnologie nel corso di un procedimento penale, previste dal Regolamento, determini o meno la loro "emarginazione" dal procedimento penale, quantomeno a far data dal momento di effettiva applicabilità delle diverse Sezioni che compongono il complesso *corpus* normativo.

A tale quesito occorre fornire una risposta indubbiamente positiva, per ragioni del tutto analoghe a quelle già esposte a proposito della contrarietà delle tecnologie in discorso con i diritti fondamentali della persona e con le disposizioni sostanziali poste a salvaguardia di questi ultimi.

Le nuove regole europee, aventi natura *self executing*, stabiliscono in quali casi e a quali condizioni il ricorso a tali sistemi di intelligenza artificiale possa considerarsi lecito alla stregua delle previsioni del Regolamento. Ne consegue che la loro violazione qualifichi come vietato dalla disciplina europea l'impiego di tali tecnologie in termini non compatibili con la suddetta regolamentazione. Divieto che, a sua volta e proprio alla luce dell'inquadramento di tali ritrovati tecnologici quali mezzi di prova o strumenti di indagine atipici, ne preclude tanto l'ammissione e l'utilizzabilità probatoria, tanto l'impiego con finalità puramente investigative, proprio sulla scorta dell'impostazione ermeneutica introdotta dalla già citata decisione delle Sezioni unite nel caso Prisco.

La seconda indicazione desumibile dalla recente legislazione europea è che risulta più che mai urgente per i legislatori nazionali in genere, tanto più per quello italiano, una esplicita "scelta di campo", a favore o contro l'impiego dell'intelligenza artificiale nei procedimenti penali. L'alternativa è manichea: vietare il ricorso a tali tecnologie, oppure elaborare una disciplina positiva in grado di delineare "percorsi procedimentali"

– necessariamente conformi alla normativa europea, di nuova introduzione – sufficientemente dettagliati, tali da restituire agli operatori del diritto un quadro di certezze in ordine a prospettive, limiti e modalità di impiego di tali ritrovati tecnologici.

È indubbio, del resto, che le articolate disposizioni intertemporali previste dal Regolamento, volte a differire la cogenza delle disposizioni più qualificanti la normativa sin qui sommariamente passata in rassegna, siano finalizzate a consentire agli Stati membri di dotarsi di una disciplina armonica alle previsioni europee e, specie con riferimento alle garanzie procedurali minime da esse appena abbozzate, coerente con le peculiarità dei singoli sistemi giuridici.

10. *Riflessioni conclusive*

Le considerazioni sin qui svolte conducono a ritenere, *de iure condito*, le tecnologie di *facial recognition* non utilizzabili nel contesto dell'accertamento penale, tanto in ambito probatorio quanto investigativo.

Tale conclusione appare, tuttavia, segnare il passo dinanzi non soltanto alla progressiva informatizzazione del processo penale ma, soprattutto, all'ampia diffusione e all'estensivo ricorso alle tecnologie informatiche nella vita quotidiana. Prassi che, com'è facile intuire, tende a "desensibilizzare" anche l'operatore del diritto rispetto alle implicazioni che l'uso di simili tecnologie comporta sul piano del rispetto dei diritti individuali.

Non può, inoltre, sfuggire come le potenzialità euristiche di tali strumenti mal si concilino con la rigida "chiusura" che l'attuale stato della disciplina processuale restituisce.

Affermazione che deve intendersi riferita sia al legittimo interesse della autorità inquirenti a servirsi di questi per la ricerca e l'individuazione del colpevole, sia all'altrettanto legittima aspettativa del difensore di ricorrere alle medesime tecnologie, allorché suscettive di condurre all'acquisizione di prove potenzialmente liberatorie.

Si tratta di forze che potrebbero spingere la giurisprudenza a ricercare soluzioni interpretative eterodosse e corrosive dei diritti fondamentali e dei complessi equilibri che governano il sistema delle prove penali, allo scopo di ridurre lo iato che separa le regole del processo dall'impetuoso sviluppo tecnologico che caratterizza i nostri tempi e che ha, già, irrimediabilmente trasfigurato la vita sociale. Rischio che appare finanche troppo facile pronosticare, specie se si tiene conto dei già segnalati "sbanda-

menti" del diritto vivente che hanno legittimato il ricorso a una vasta congerie di "ricognizioni" irrituali, in evidente violazione del principio di legalità della prova[96].

Non si trascuri, peraltro, di considerare come le, pur cospicue, previsioni europee di recente introduzione, tanto con riferimento ai sistemi di riconoscimento facciale operanti in tempo reale tanto a posteriori, non vietano affatto la loro possibilità d'impiego, specie in ambito investigativo. Esse prevedono sì un ampio novero di requisiti e di condizioni di legittimità dell'uso di simili ritrovati tecnologici ma, al contempo, sono contraddistinte da un notevole tasso di genericità e corredate da numerose previsioni derogatorie. In altre parole, anche tenuto conto della natura dell'atto-fonte dalle quali esse discendono, le disposizioni del Regolamento non paiono delineare una disciplina sufficientemente stringente e in grado di "resistere" a possibili tentativi di aggiramento.

Lo conferma, ad esempio, il tenore dello stesso art. 26 paragrafo 10 già citato, il quale esclude espressamente dal novero degli usi non consentiti, in difetto di apposita autorizzazione o convalida da parte dell'autorità giudiziaria, l'impiego di sistemi di intelligenza artificiale finalizzati «all'identificazione iniziale» di un possibile sospettato.

Occorre, dunque, che il legislatore intervenga al più presto, predisponendo una disciplina positiva in grado di contemperare gli opposti interessi e valori in rilievo, nonché di adeguare la disciplina processuale interna alle disposizioni e alla cornice regolamentare di matrice euro unitaria.

Tale obiettivo, di certamente non agevole conseguimento, richiede, tuttavia, la ricerca di soluzioni innovative che tengano conto non solo dell'esigenza di tutela dei dati biometrici oggetto di trattamento ma, soprattutto, della necessità di presidiare il complesso equilibrio di pesi e contrappesi che caratterizza il processo penale e, in modo particolare, i rapporti tra indagini e dibattimento.

In questo contesto un rilevantissimo ostacolo all'impiego probatorio di tali strumenti è posto dalla già richiamata «opacità algoritmica» che li caratterizza e che restituisce l'immagine di una *black box* produttiva di risultati di conoscenza non adeguatamente controllabili e verificabili dal giudice[97].

Constatazione che, tuttavia, dovrà necessariamente essere aggiornata e ulteriormente verificata dopo che la disciplina europea relativa ai requi-

[96] Sul punto, v. *retro, sub* 2.
[97] Sul punto, v. *retro, sub* 5.

siti di immissione in commercio, distribuzione e utilizzo di tali ritrovati avrà ricevuto compiuta attuazione e implementazione.

Ad acuire la dimensione problematica del compito che spetta al legislatore concorre non solo la dubbia idoneità epistemologica dei moderni *software* di *facial recognition* ma, altresì, il rischio che il giudice possa essere indotto dalla consultazione di uno strumento tecnologico "intelligente" (ma i cui concreti processi cognitivi non è in grado di comprendere) e apparentemente "neutrale" a ricorrere a una sorta di fideistico e, dunque, acritico affidamento ai risultati di conoscenza proposti dalla "macchina"[98]. Tanto alla stregua di una sorta di novella "prova legale" del tutto inconciliabile con il vigente modello processuale, imperniato sul contraddittorio nella formazione della prova e sul libero (ma motivato) convincimento.

Non pare, allora, azzardato suggerire al futuro legislatore di prendere in considerazione una soluzione compromissoria, da ravvisarsi nella predisposizione di una disciplina normativa armonica con le previsioni europee, idonea a legittimare il ricorso a tali tecnologie esclusivamente nel corso delle indagini preliminari e con scopi puramente investigativi, sancendone al contempo e senza eccezioni l'inutilizzabilità probatoria. In altre parole, quel che si auspica è una sorta di implementazione dell'intelligenza artificiale in ambito penale esclusivamente quale sussidio investigativo, alla stregua di una versione tecnologica dell'informatore di polizia, irrinunciabile in qualsivoglia sistema penale, ma al contempo radicalmente insuscettibile di impiego probatorio alcuno.

Un simile congegno consentirebbe di contemperare le esigenze investigative e quelle probatorie, senza né rinunciare aprioristicamente alle potenzialità conoscitive rese disponibili dalle moderne tecnologie né dare ingresso nel dibattimento a fonti di prova non adeguatamente verificabili. Accedendo a una simile proposta, resterebbe da stabilire se i risultati di conoscenza ottenuti attraverso il ricorso a tali strumenti possano costituire il fondamento di decisioni incidentali, quali l'applicazione delle misure cautelari. Tema rispetto al quale, impregiudicata l'esigenza di riflessioni più approfondite, parrebbe logico esprimersi in senso negativo, tenuto

[98] Un rischio che, del resto, sia pure con diverse accentuazioni, pare essere stato sottolineato anche dalla dottrina, nel rilevare la possibilità che «l'ingresso nel circuito giudiziale degli strumenti informatici e delle macchine (più o meno) intelligenti gener[i] forme di inedita deresponsabilizzazione degli attori processuali, in particolare del giudice». In tal senso, per tutti, L. Luparia Donati, *La promessa della giustizia tecnologica*, in *Sistema penale*, 1 agosto 2024, 2.

conto della dimensione schiettamente prognostica – e, dunque, proiettata verso il possibile esito del successivo giudizio dibattimentale – dell'accertamento incidentale sul *fumus commissi delicti* richiesto in sede di applicazione di una misura limitativa della libertà.

Un simile approccio alla materia richiederebbe, però e al contempo, un penetrante sforzo di rivisitazione critica da parte della giurisprudenza degli orientamenti interpretativi che si sono, sin qui, impegnati in un'opera di progressiva ma inesorabile erosione della centralità dell'istituto della ricognizione quale unico mezzo di prova tipico suscettivo di garantire l'individuazione e il riconoscimento di persone nel contesto dell'istruzione dibattimentale[99].

Sarebbe, difatti, del tutto incoerente sul piano sistematico introdurre una specifica regola di esclusione in ambito probatorio delle tecnologie di riconoscimento facciale, lasciando al contempo libera la giurisprudenza di seguitare a legittimare prassi quali il riconoscimento di persona effettuato dal testimone nel corso dell'esame dibattimentale o, a maggior ragione, la semplice conferma del riconoscimento fotografico operato dal dichiarante nel corso della fase preliminare[100].

Occorre, dunque, una esplicita revisione degli orientamenti esegetici ormai consolidatisi nel diritto vivente o, in alternativa, un intervento legislativo *ad hoc*, teso a ribadire quanto, in verità, dovrebbe risultare già ovvio sul piano sistematico e interpretativo, ovverosia che il riconoscimento di persone nel dibattimento penale possa e debba avvenire esclusivamente nelle forme previste dagli artt. 213 ss. c.p.p., dovendo ogni deviazione rispetto al modello legale essere derubricata a prova assunta in violazione della legge processuale e, perciò, inammissibile o inutilizzabile.

In definitiva, appare pressante l'esigenza di un "chirurgico" ma meditato intervento legislativo, al fine di scongiurare che l'attuale situazione di sostanziale "anomia" (quantomeno sul piano della legislazione interna e, in particolare, di quella processuale) possa, alternativamente, condurre a insidiose deviazioni dalla rigorosa interpretazione delle regole e dei principi della procedura penale, suscettivi di riverberare sui diritti individuali e sulla correttezza epistemologica dell'accertamento, ovvero seguitare a restituire l'impressione di una anacronistica "chiusura" del sistema di giustizia penale a tecnologie di larghissimo impiego e dalle innegabili potenzialità sul piano della ricostruzione dei fatti di rilievo processuale.

[99] Sul punto, v. *retro, sub* 2.
[100] Sul punto, v. *retro, sub* 2.

Fulvio Costantino

SICUREZZA SOCIALE E DISCRIMINAZIONE SOCIALE

1. *Introduzione*

Il tema della sicurezza, in senso lato, è alla base anche del ricorso a modalità di cd. *social credit scoring*[1]. Le autorità pubbliche possono infatti valutare l'affidabilità sociale dei cittadini attribuendo loro un punteggio, sulla base della valutazione di alcuni parametri, tra cui le caratteristiche della personalità, il comportamento sociale, la rete di relazioni. Il punteggio finisce così per quantificare il valore sociale e la reputazione di un soggetto.

Dei sistemi di reputazione nel settore pubblico si discute dall'ultimo decennio del precedente secolo, e ciò avviene con l'intento di contrastare fenomeni illeciti quali corruzione, frodi e violazioni degli obblighi contrattuali. Lo *scoring* si è diffuso anzitutto nell'ambito privato ed è il meccanismo che ha consentito al commercio *online* di affermarsi: il modello, anche dei sistemi pubblici, è costituito dai sistemi di *credit scoring* finanziari di matrice statunitense[2].

[1] www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9778361.

[2] Sul tema si vv., nella dottrina italiana: L. Ammannati - G.L. Greco, *Il credit scoring "intelligente": esperienze, rischi e nuove regole*, *Rivista di diritto bancario*, 2023, 461; N. Brutti, *Mito del consenso e rating reputazionale*, *Nuova giurisprudenza civile commentata*, 2024, 402; G. Cerrina Ferroni, *Intelligenza artificiale e sistemi di scoring sociale. tra distopia e realtà*, *Diritto dell'Informazione e dell'Informatica*, 2023, 1; E. Consiglio - G. Sartor, *Il sistema di credito sociale cinese: una «nuova» regolazione sociotecnica mediante sorveglianza, valutazione e sanzione*, *Tigor: rivista di scienze della comunicazione e di argomentazione giuridica*, 2021, 139; F. Costantini - G. Franco, *Decisione automatizzata, dati personali e pubblica amministrazione in Europa: verso un "Social credit system"?*, *Istituzioni del federalismo*, 2019, 715; D. Di Sabato - G. Alfano, *L'impiego dell'IA per condizionare e valutare le persone tra limitazioni e divieti: qualche considerazione critica sulla proposta*

I meccanismi di reputazione mirano a incentivare l'adozione di comportamenti virtuosi, e per l'effetto di far convergere i comportamenti verso la normalità statistica. Essi operano sulla base o di strumenti di punizione, in quanto i soggetti non virtuosi vengono iscritti in liste cd. nere, o di ricompensa, allorché i soggetti virtuosi vengono iscritti in liste cd. rosse, o ancora sulla base di indici di punteggio, che rappresentano una miscellanea dei due sistemi.

Si viene a configurare, nell'ottica dell'impiego pubblico di questi strumenti, una sorta di «cittadinanza a punti», che, si è osservato, si traduce in una cd. ludicizzazione della cittadinanza[3], che però ha rilevanti conseguenze giuridiche su diritti e libertà degli interessati, inclusi i soggetti più vulnerabili[4].

Tali meccanismi sono espressione di un progetto generale di controllo dei cittadini, che ha – e mira ad avere – un impatto sulla costruzione della personalità, e che rischia di comportare limitazioni della libertà e di bandire le espressioni di eccentricità: per evitare sanzioni, che siano licenziamenti o semplici privazioni di opportunità, o per conseguire ricompense, di fatto sono indotti atteggiamenti di sottomissione e comportamenti conformisti; viene inoltre incentivato un atteggiamento di com-

di Regolamento sull'IA elaborata dalla Commissione europea, *Rivista di diritto dell'impresa*, 2022, 281; F. D'Orazio, *Il "credit scoring" e l'art. 22 del GDPR al vaglio della Corte di giustizia*, *La Nuova Giurisprudenza Civile Commentata*, 2024, 410; V. Pietrella - S. Racioppi, *Il credit scoring e la protezione dei dati personali: commento alle sentenze della Corte di giustizia dell'Unione europea del 7 dicembre 2023*, *Rivista italiana di informatica e diritto*, 2024, 175; M. Rabitti, *Discriminazioni tecnologiche e Fin-tech*, *Rivista di diritto dell'impresa*, 2023, 467; M. Sciacca, *Algocrazia e sistema democratico. Alla ricerca di una mite soluzione antropocentrica*, *Contratto e impresa*, 2022, 1173; G. Sciascia, *Reputazione e potere: il social scoring tra distopia e realtà*, *Giorn. dir. amm.*, 2021, 317.; A. Vigorito, *Sul crinale tra data altruism e social scoring: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo*, *Medialaws*, 2023, 104. Lo studio più completo sul tema è di E. Di Carpegnia Brivo, *Pari dignità sociale e Reputation scoring. Per una lettura costituzionale della società digitale*, Torino, 2024, preceduto da *Il Reputation scoring e la quantificazione del valore sociale*, *Federalismi.it*, 2022, 119.

Nel caso italiano del credit scoring finanziario, si rimanda allo Studio della Banca d'Italia N. 721 - *Intelligenza artificiale nel credit scoring: analisi di alcune esperienze nel sistema finanziario italiano* 2022 che ha evidenziato come l'adozione di modelli di intelligenza artificiale per la valutazione dei rischi incrementi il numero di distorsioni e di discriminazioni.

[3] T. Fray, *Should we Gamify Citizenship in the Metaverse?*, *futuristspeaker.com*, 2022.

[4] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9778361, *cit*.

petizione, che può produrre stress, comportare perdita di autostima e stimolare atteggiamenti di rinuncia.

Il problema si pone anche nei casi in cui l'adesione a questi programmi di controllo sia volontaria: la prospettiva di un premio, anche modesto, favorisce la prestazione del consenso a profilazioni anche molto penetranti, e del resto il sistema, sia nella prospettiva premiale che punitiva, è efficace proprio quando incide sull'accesso a beni e servizi di consumo[5].

Va segnalata inoltre in questa attività di profilazione una stretta relazione tra sfera pubblica e privata: i cittadini sono spesso controllati sia nelle attività pubbliche che private, così come i premi spesso sono forniti da attori pubblici e privati.

2. *Il SCS cinese*

Vi è un riferimento ricorrente a tal proposito al SCS (*social credit scoring*) cinese, il quale mira a incentivare la sincerità, l'onestà e l'integrità e punire le devianze, per il perfezionamento e la regolamentazione dell'economia di un mercato socialista, attraverso l'eliminazione delle patologie del mercato, come truffe e contraffazioni, e la promozione della affidabilità finanziaria all'interno e da parte del mercato cinese[6].

[5] A differenza di un obbligo o di un divieto, il termine "volontario" perde rapidamente il suo significato quando il costo sociale o finanziario dell'opt-out diventa troppo elevato: B. VON WYL, *Are social scoring systems a threat to democracies?*, https://www.swissinfo.ch/eng/digital-democracy/are-social-scoring-systems-a-threat-to-democracies/89576473.

[6] Sul caso cinese, L. Esposito, *La protezione dei dati personali nel panorama giuridico cinese. Analogie con il GDPR?*, *Comparazione e diritto civile*, 2023, pp. 1095; M. Burnay - E. Pils, *Weaponizing Citizenship in China: Domestic Exclusion and Transnational Expansion*, *State Crime Journ.*, 2020, 4; A. De Jonge, *A Relational Governance Perspective on the Politics of China's Social Credit System for Corporations*, *Hastings Int'I & Comp. L. Rev.*, 2021, 111; B. Honghai, *Old Regulatory Wine in a New Bottle of Technology - A Critical Analysis of China's Social Credit System*, *Univ. Penns. Asian Law Rev.*, 2021, 282; J. Pabisiak, *Dangerous, Yet Not So Unique. Characteristics of the Chinese Social Credit System*, *Pol. Pol. Sc. Yearb.*, 2020, 3 30; L. Rettinger, *The Human Rights Implications of China's Social Credit System*, *Journ. High Techn. Law*, 2021, 1; K. Werbach, *Orwell That Ends Well? Social Credit as Regulation for the Algorithmic Age*, *Univ. Illin. Law Rev.*, 2022, 1417; Z. Wenyan, *On the Legal Issues of Chinese Social Credit System*, *China Legal Science*, 2021, 4, 3.

Il Sistema di Credito Sociale è coordinato dal "Gruppo Dirigente Centrale per l'Approfondimento di Riforme Comprensive". Secondo la "Pianificazione della Creazione del Sistema di Credito Sociale (2014-2020)", pubblicata dal Consiglio di Stato nel 2014, esso

Per il Consiglio di Stato cinese il *Social Credit Scoring* (SCS) costituisce una componente fondamentale dell'economia di mercato socialista e della 'governance' sociale, che concorre a creare una «cultura della sincerità», incoraggia la «fiducia» e consente di costruire una «armoniosa società socialista»[7].

Esso è stato oggetto di numerose critiche per come sia stato plasmato per la realizzazione di un progetto totalitario: si è rilevato infatti che il *rating* sociale sarebbe stato collegato al corretto pagamento delle tasse, alla partecipazione a organizzazioni invise al governo[8], alla frequentazione, anche per ragioni di lavoro, di persone con un *rating* sociale basso. Al punteggio alto sarebbero stati di conseguenza correlati l'accesso facilitato a finanziamenti, affitti o noleggi, agevolazioni degli spostamenti, il miglioramento dello *status* sociale[9]; a un *rating* sociale troppo basso sarebbero conseguiti, per nove milioni di persone, tra l'altro, la impossibilità di acquistare biglietti aerei per voli domestici o viaggiare su treni ad alta velocità[10].

riguarda quattro aree: "onestà negli affari di governo", "integrità commerciale", "integrità sociale" e "credibilità giudiziaria" *(https://digichina.stanford.edu/work/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/)*.

[7] Esso è previsto dal documento programmatico nazionale «Schema di pianificazione per la costruzione di un sistema di credito sociale (2014-2020)». Il Consiglio di Stato ha pubblicato nel 2019 «Pareri guida sull'accelerazione della costruzione di un sistema di credito sociale e sulla costruzione di un nuovo meccanismo di vigilanza basato sul credito» e ha sottolineato la necessità che i big data e l'intelligenza artificiale forniscano un allarme tempestivo di attori rischiosi che necessitano di maggiore attenzione normativa. Nel dicembre 2020 è stata messa in consultazione interna una bozza di Legge sul Credito Sociale. Il piano quinquennale del giugno 2022 per lo «stato di diritto», le indicazioni del Consiglio di Stato e un progetto di legge presentato nel novembre 2022 hanno confermato la volontà di implementare il sistema, in particolare legittimando i regolamenti esistenti implementati a livello locale, come quello di Shanghai (Donnelly, op. cit.).

[8] Alle violazioni legate alla raccolta differenziata dei rifiuti, al comportamento alla guida, alle visite ai genitori anziani, alla correttezza dell'attraversamento pedonale, dell'uso del guinzaglio per i cani, dell'uso della mascherina, dell'uso di sigarette in zone per non fumatori, del tempo speso e del comportamento assunto su internet o nei videogiochi, fino all'atteggiamento di critica al partito.

[9] La lista nera più rilevante è la Lista delle persone disoneste soggette a esecuzione della Corte Suprema del Popolo (http://gongbao.court.gov.cn/Details/1c0baa9e69e6a21c809886144354b1.html), Secondo le statistiche ufficiali, dalla sua promulgazione nel 2013 alla fine del 2018, quasi 13 milioni di individui sono stati inseriti nella Lista delle persone disoneste (http://en.people.cn/n3/2019/0303/c90000-9551837.html).

[10] Ottenere prestiti dalle banche, vivere in determinati quartieri, ottenere determinati lavori, acquistare beni di lusso, far frequentare ai figli determinate scuole, affittare camere in hotel di lusso, usare carte di credito, ottenere lavori prestigiosi, avere una connes-

Si è tuttavia replicato che non si sarebbe realizzato alcun sistema di credito sociale comprensivo ed esteso a tutta la nazione, anche per ragioni tecniche[11]; che sarebbero solo avvenute delle sperimentazioni a livello regionale e locale, e solo queste ultime avrebbero creato maggiore scalpore presso l'opinione pubblica occidentale[12].

sione *internet* veloce. I casi sono elencati negli articoli di cui s*upra*, si vv. anche, a livello giornalistico, Z. YANG, *How China's social credit system actually works – it's probably not how you think*, *Post Magazine*, 2023, www.scmp.com/magazines/post-magazine/long-reads/article/3205829/how-chinas-social-credit-system-actually-works-its-probably-not-how-you-think, D. DONNELLY, *China Social Credit System Explained – What is it & How Does it Work?*, 2023, Horizons, nhglobalpartners.com/china-social-credit-system-explained/, V. BRUSSEE, *China's social credit score – untangling myth from reality*, 2022 https://merics.org/en/opinion/chinas-social-credit-score-untangling-myth-reality.

[11] Il sistema nel suo complesso è poco digitalizzato, altamente frammentato (Z. WENYAN, On the Legal Issues, cit., 21). Attualmente vi è una serie di liste basate su vari tipi di violazioni, controllate da agenzie non coordinate tra loro (DONNELLY, op. cit. nel paragrafo Blacklists and Redlists in the Chinese Social Credit System).

Si è anche osservato come non vada enfatizzato il ruolo politico del CSC, in quanto esistono già molti strumenti segreti con cui colpire i dissidenti (BRUSSEE, op. cit.). Non c'è inoltre attualmente uso dell'intelligenza artificiale (YANG, op. cit.), non ci sono sanzioni attribuite in maniera automatica (B. HONGHAI, Old Regulatory Wine, cit., 321).

[12] Risalgono al 2009 i progetti pilota regionali del sistema di credito sociale, a cui si sono aggiunti i progetti nelle città (2017). Tra questi i più noti sono quelli della contea di Suining, provincia di Jiangsu: le condanne o il mancato rimborso del debito, così come alcuni commenti online comportavano detrazioni di punti e il punteggio avrebbe influito sulle opportunità di lavoro, sull'accesso alle licenze commerciali e sull'idoneità al sostegno del governo. A Nanchino nel 2016 gli istituti finanziari offrivano ai soggetti con punteggi più alti sconti e trattamenti preferenziali, rilasciati anche sulla base della disponibilità a donare il sangue e sulla valutazione delle prestazioni lavorative. La città di Rongchen prevedeva la collaborazione tra 142 dipartimenti e includeva centinaia di fattori per determinare il punteggio abilitativo di accesso prioritario a finanziamenti e licenze, tra cui la diffusione di informazioni dannose su *chat*, *forum* e *blog* o la vittoria di una competizione sportiva o culturale a livello nazionale, il corretto attraversamento pedonale o smaltimento dei rifiuti, la donazione del sangue o la stravaganza del matrimonio, con la conseguenza di *trattamenti preferenziali nei servizi pubblici come ricompensa o la sospensione dei sussidi come sanzione (https://www.chinalawtranslate.com/en/rongcheng-municipal-personal-credit-appraisal-standards/).*

A Suzhuo il punteggio è stato applicato a 13 milioni di residenti, detraendo punti anche per gli imbrogli nei giochi *online* (tutte le informazioni in Donnelly, op. cit.).

I governi locali hanno effettuato una sperimentazione talvolta audace, con una commistione anche di credito sociale e finanziario; a livello nazionale l'approccio è stato quello di mantenere i due separati, con diverse regole (B. HONGHAI, *Old Regulatory Wine*, *cit.*, 294).

I governi locali hanno incontrato problemi nel rendere operativi i sistemi di credito sociale, tra cui la presenza di *silos* di dati, *standard* incoerenti e resistenze burocratiche,

Il sistema è stato modificato sulla base dell'esperienza[13]: l'attenzione risulta incentrata sull'implementazione dello stesso principalmente al controllo aziendale[14]. I metodi di classificazione individuali locali sono stati posti in stallo: tuttavia, sebbene non esista comunque un sistema unificato nazionale che assegni un punteggio unico a ogni persona, e i

per cui molti non sono riusciti nemmeno a superare il primo passaggio, costituito dalla condivisione dei dati tra i dipartimenti.

Molti progetti pilota e programmi inoltre sono stati criticati dai *media* e, laddove basati su punti per indirizzare il comportamento al di là di quanto richiesto dalla legge, sono stati interrotti o limitati alla partecipazione volontaria (Brussee, *cit.*).

Dal 2019 le autorità centrali cinesi hanno fornito dei pareri guida chiarimenti formali sul fatto che i punteggi non potevano essere utilizzati per penalizzare i cittadini e che solo documenti legali formali potevano fungere da motivo di sanzioni, così standardizzando il tipo di informazioni che possono essere registrate nell'ambito del credito sociale, nonché la gamma di misure disciplinari. Si è precisato che tutte le sanzioni devono avere una base giuridica nella legislazione nazionale e solo le violazioni gravi possono essere inserite nella lista nera. (*https://www.ndrc.gov.cn/xxgk/zcfb/ghxwj/202212/t20221230_1345067.html*).

Le città pilota hanno seguito le indicazioni. Wenzhou ha modificato i programmi e pubblicato uno schema con misure promozionali; Rongcheng nel 2021 ha previsto un'applicazione volontaria e solo ricompense. Weihai ha deciso di escludere dal sistema di punteggio i dati relativi all'attraversamento pedonale, al rispetto del codice della strada e al corretto pagamento delle tariffe di parcheggio. Suzhou ha deciso di non penalizzare i videogiocatori. Le iniziative che sopravvivono prevedono perciò solo incentivi positivi. L'equilibrio si è stabilito ammettendo premi extralegali, laddove invece le sanzioni devono essere legate alla violazione della legge (*ibidem*).

[13] Il sistema nazionale però imporrà elementi tecnologici, per mettere in comune i dati, se le agenzie vogliono applicare sanzioni sulla base di dati di altre agenzie (*ibidem*). I colossi della tecnologia non sono coinvolti nel fornire dati o compilare valutazioni del credito, ma si sono preoccupati a seguito a seguito di infrazioni di legge punire sulla piattaforma (Yang, *op. cit.*).

Il sistema in particolare si concentra sulle aziende, e ha riguardato più di 33 milioni di imprese (Donnelly, *op. cit.*): in questa ottica il SCS *è uno strumento meccanismo di regolazione del mercato, in quanto le aziende si conformano alle politiche e alle disposizioni del Governo, dal momento che con punteggi alti avranno migliori condizioni sui prestiti, tasse più basse, più opportunità, in quanto potranno partecipare a progetti finanziati dal settore pubblico.* L'azienda in una lista rossa, in quanto virtuosa, gode di procedure amministrative semplificate, meno ispezioni governative e *audit*, approvazioni veloci (K. Werbach, *Orwell That Ends Well?*, *cit.*, 1470). Di converso, le aziende possono essere inserite in una lista nera a causa di particolari violazioni. Non è esclusa la possibilità che anche le imprese straniere che operano in Cina siano sottoposte alla classificazione all'interno del sistema.

[14] In ordine a questo profilo, sarebbero oggetto di attenzione il comportamento finanziario e la supervisione aziendale, ma con un monitoraggio delle inadempienze giudiziarie e con maggiore spazio a premi e a forme di riabilitazione.

cittadini è previsto subiscano sanzioni per violazioni legali, non per comportamenti personali quotidiani[15], il processo non si è arrestato[16].

In questa direzione si pongono anche le nuove linee guida del marzo 2025, che per un verso si concentrano sulle aziende, con un'attenzione particolare per alcuni settori strategici[17], per altro verso, e soprattutto,

[15] La Cina ad oggi non dispone di un sistema di credito sociale standardizzato a livello nazionale che valuti ogni cittadino e gli assegni un punteggio. Le liste nere sono per la stragrande maggioranza elenchi di soggetti che si rifiutano di ripagare i debiti o gli stipendi dovuti.

Alla fine del 2020 il governo centrale ha iniziato a "ricentralizzare" il sistema di credito sociale (https://platform.wirescreen.ai/organization/87822355-b26c-5487-8511-3c-2d9a68e989).

L'impressione che si ricava è di un interesse ad attuare il sistema di credito sociale soprattutto in chiave commerciale, per monitorare le aziende.

[16] Si v. M. Chen - J. Grossklags, Algorithmic regulation at the city level in China, Data Policy, 21 April 2025

https://www.cambridge.org/core/journals/data-and-policy/article/algorithmic-regulation-at-the-city-level-in-china/57D30B18C3A50C7208B3E6DFF88BBC74. Lo studio mette in evidenza come, a differenza dei sistemi di punteggio creditizio pubblici aziendali, che enfatizzano sia le punizioni che le ricompense, i sistemi di punteggio creditizio personale nelle città si concentrino prevalentemente sulle ricompense. Le misure di penalizzazione associate a punteggi bassi per gli individui spesso non vengono menzionate. Le misure di ricompensa per i punteggi creditizi personali vengono divulgate, ma in modo piuttosto generale. I servizi pubblici solitamente coprono l'assistenza sanitaria (trattamento prima e pagamento dopo), il parcheggio (sconti) e l'uso della biblioteca (senza deposito), mentre i servizi commerciali possono includere i viaggi (sconti per i biglietti d'ingresso a luoghi panoramici) e la ricerca di lavoro (il sistema segnala un'istruzione verificata e un background professionale).

Le amministrazioni locali stanno esplorando la fattibilità di istituire un meccanismo di riconoscimento reciproco attraverso la condivisione delle informazioni. Questa tendenza implica che il futuro dei sistemi di punteggio creditizio personale potrebbe continuare a evolversi in modo frammentato, sebbene con l'introduzione di meccanismi di riconoscimento reciproco. Si osserva che quindi vi potrebbe essere una regolamentazione algoritmica per il controllo sociale a livello nazionale senza la necessità di un unico SCS unificato.

[17] Il 31 marzo 2025 l'Ufficio Generale del Comitato Centrale del Partito Comunista Cinese e l'Ufficio Generale del Consiglio di Stato hanno pubblicato le nuove Linee Guida per il Miglioramento del Sistema di Credito Sociale.

Il documento mira a promuovere l'integrazione di norme tra istituzioni pubbliche, imprese private, organizzazioni sociali e individui, per rafforzare fondamenti giuridici, standard di trasparenza e l'applicabilità del sistema creditizio.

Le nuove linee guida inaspriscono i controlli contro i comportamenti disonesti delle aziende: le aziende classificate come gravemente disoneste saranno soggette al divieto di accesso a fondi governativi, incentivi fiscali e offerte di titoli. Si istituiscono liste nere

minano ad affrontare le critiche di arbitrarietà del sistema sottolineando la necessità che le misure siano proporzionate, fondate sulla legge e che i comportamenti "disonesti" siano disciplinati da leggi e regolamenti e correttamente classificati[18]. Un altro aspetto interessante è la previsione di condivisione transfrontaliera dei dati, nell'ottica della promozione di questo sistema come *standard* globale[19].

3. *Le esperienze straniere*

La raffigurazione che si fa del Sistema di Credito Sociale cinese si riferisce al progetto di fornire un unico punteggio comprensivo dei diversi aspetti della vita di un individuo; si è osservato che nelle società occidentali i sistemi di valutazione dovrebbero guardare ai cittadini come "dividui" (cd. *dividuals*), affinché ogni sistema di valutazione sia confinato a singoli ambiti e sui soli dati ad essi pertinenti[20].

specifiche per settore, per una maggiore vigilanza nei settori immobiliare, dei servizi *internet*, delle risorse umane e dell'energia.

Gli stessi dipartimenti governativi sono ora soggetti a valutazioni del merito creditizio e si formalizza l'istituzione di un elenco di "entità gravemente screditate".

https://www.china-briefing.com/news/china-social-credit-system-dishonest-consequences-2025/

[18] I meccanismi di applicazione devono avere fondamento giuridico, essere trasparenti e le sanzioni devono essere standardizzate, eque e proporzionate, adeguate alla gravità della violazione, evitando misure arbitrarie o eccessivamente punitive.

Si richiedono per l'implementazione del sistema una migliore condivisione delle informazioni, e una solida protezione dei dati personali, quest'ultima in particolare per limitare la raccolta eccessiva di dati e vietare il trattamento o la vendita illegale di informazioni personali.

Si sottolinea l'importanza di una classificazione accurata dei comportamenti disonesti, con elenchi specifici per settore, con particolare attenzione per quello immobiliare, dei servizi *internet*, delle risorse umane e dei contratti energetici a lungo termine.

Le misure disciplinari devono essere basate su leggi e regolamenti, senza il cui fondamento nessuna azione punitiva, come l'inserimento in liste nere o la limitazione dell'accesso alle risorse pubbliche, può essere applicata. Le autorità sono tenute a definire con precisione la classificazione dei comportamenti disonesti, distinguendo tra infrazioni generali e gravi.

[19] La cooperazione transfrontaliera in materia di condivisione dei dati creditizi riguarda in particolare i paesi BRICS e i partecipanti alla *Belt and Road Initiative*. Si mira a istituti di *rating* del credito competitivi a livello globale e al riconoscimento reciproco dei prodotti creditizi.

[20] F. Lagioia - G. Sartor, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, *Federalismi.it*, 2020, 85, in part. 107.

In questo senso, tra i due poli del mero *credit scoring* basato su dati relativi al solo settore di riferimento e il *social credit scoring* che scrutina tutti gli aspetti della vita, si può però porre una zona grigia nella quale sono rinvenibili diverse combinazioni[21].

Per un verso, attori privati si servono di informazioni esterne che contribuiscono alla valutazione: compagnie specializzate in assicurazioni sulla vita a New York sono state autorizzate ad utilizzare le informazioni reperite nei *social network* per decidere in ordine ai contratti da stipulare[22].

Per altro verso, soggetti pubblici utilizzano strumenti di *social credit* per attuare le proprie politiche: diversi enti locali hanno sviluppato iniziative con scopo premiale associate all'adozione di comportamenti «virtuosi» dei cittadini in diversi settori (ambiente, fiscalità, cultura, mobilità, *sport*)[23]: si tratta peraltro di progetti generalmente caratterizzati da forme

[21] Nell 2022 in Canada, il presidente ha utilizzato i poteri di emergenza per congelare i conti bancari degli autotrasportatori che bloccavano il traffico in entrata e in uscita dagli Stati Uniti (https://www.tempi.it/camionisti-terroristi-trudeau-canada/). In Svizzera un software permetteva agli insegnanti di segnalare i propri studenti come potenziali terroristi; il sito web è stato poi disattivato (L'esempio è citato in https://www.swissinfo.ch/eng/digital-democracy/are-social-scoring-systems-a-threat-to-democracies/89576473 e il sito è https://www.begs.ch/angebot/ra-prof/).

[22] https://www.wsj.com/articles/new-york-insurers-can-evaluate-your-social-media-useif-they-can-prove-why-its-needed-11548856802; https://www.forbes.com/sites/nizangpackin/2019/12/13/social-credit-much-more-than-your-traditional-financial-credit-score-data/; https://protectyourwealth.ca/can-social-media-activity-impact-your-life-insurance-ratescan-social-media-activity-impact-your-life-insurance-rates/

N. Pang, *Your Phone Already Has Social Credit. We Just Lie About It.*, https://www.thenexus.media/your-phone-already-has-social-credit-we-just-lie-about-it/ osserva come gli istituti di credito specializzati analizzino i profili dei *social media* per la valutazione del credito, in particolare per i soggetti con una storia creditizia limitata; le *app* di pagamento e i servizi finanziari monitorano i modelli di spesa e i comportamenti relativi alle transazioni per creare profili di rischio; la Banca Centrale Europea ha chiesto ad alcune istituzioni di monitorare le conversazioni sui *social media* per individuare tempestivamente possibili assalti agli sportelli bancari, sebbene ciò riguardi il rischio sistemico e non i singoli conti; LinkedIn gestisce la visibilità professionale in base ai modelli di coinvolgimento, alla frequenza di pubblicazione e alle connessioni di rete, e su queste classifiche i reclutatori fanno affidamento per filtrare i candidati.

[23] S. Domezet - M. Lubura et al., *Chinese Social Credit System: New Challenges for the Right to Privacy?*, Journ. Lib. Int. Aff., 2021, 141 e L. Orgad - W. Reijers, *How to Make the Perfect Citizen*, *cit.*, 1103 sul candidato democratico alla presidenza Andrew Yang, il quale ha proposto una forma di credito sociale digitale (2020), legato a forme di impegno civico e volontariato. Entrambi i lavori riferiscono come, a livello comunale, siano sempre più numerosi i casi di credito sociale e i cataloghi comunali di «buone azioni»

di collaborazione tra pubblico e privato, in cui l'assegnazione di punteggi avviene grazie a raccolte di dati conferiti volontariamente dagli interessati. E, come anticipato, si osserva che comunque, rispetto alle possibilità di controllo sociale, la stessa distinzione tra controllore pubblico e privato tenda a essere meno netta di quanto sembri, vista l'ampiezza di possibilità e collaborazioni nelle forme di controllo[24].

Non si deve neppure pensare che vi sia una generale opposizione nei confronti di questi sistemi[25]: si è osservato che l'aumento dei livelli di sorveglianza avverrà come semplice risultato dei nostri maggiori livelli di automazione e ci si è quindi chiesti se non sia addirittura meglio creare un sistema formale in anticipo invece di lasciare che le forme di tecnolo-

da compiere per ottenere premi: votare, aiutare gli anziani, cercare una formazione professionale, seguire corsi di primo soccorso, organizzare eventi culturali, partecipare a laboratori di lavoro autonomo, attività che danno diritto a trasporto pubblico gratuito e al noleggio di biciclette, biglietti per eventi culturali e ad un accesso più facile agli alloggi comunali. Essi riferiscono inoltre di sistemi di incentivazione dell'impegno civico, della solidarietà sociale, del volontariato e dell'interazione sociale sperimentati a Barcellona (Social Coin), Cascais in Portogallo (Innowave CityPoints) e Hull nel Regno Unito (HullCoin). Nel 2020, uno studio commissionato dal Ministero tedesco della ricerca, della tecnologia e dello spazio ha ipotizzato un sistema di bonus sulla base di comportamenti virtuosi per la Germania per il 2030, per un'"ottimizzazione dei servizi pubblici basata sui dati", collegata a un sistema di democrazia diretta in cui i cittadini dovrebbero plasmare il sistema. Il sistema potrebbe innescare dei conflitti https://www.bmftr.bund.de/SharedDocs/Downloads/DE/v/zukunft-wertvorstellungen-lang.html. L'Estonia ha istituito un database nazionale, che include vari dati dei cittadini, come cartelle cliniche o titoli di studio, per facilitare diversi servizi, promuovere la trasparenza e influenzare il comportamento collettivo (Keen, Riferimento Keen2016) che rientra nell'ambizione generale di creare un portafoglio europeo di identità digitale (vedi https://e-estonia.com/estonia-the-eid-pioneer-reacts-to-the-european-digital-wallet-plans/).

[24] N. Pang, *Your Phone Already Has Social Credit. We Just Lie About It*., *cit.*, afferma che non sembra così fondata la osservazione secondo cui vi sia una differenza radicale tra il monitoraggio aziendale e la sorveglianza governativa, in quanto le aziende competono tra loro e si può cambiare servizio, perché i governi hanno un potere di monopolio e possono limitare le libertà fondamentali. Infatti i costi di passaggio tra le principali piattaforme sono enormi; i sistemi di credito sociale aziendale collaborano sempre di più tra loro; i governi occidentali accedono già a questi dati aziendali attraverso canali legali e acquisti di dati.

[25] L. Orgad, W. Reijers, *How to Make the Perfect Citizen*, *cit.*, 1101 compara il modello cinese con quelli occidentali: Il sistema cinese valuta le persone come cittadini, non le prestazioni rispetto alla professione svolta o al ruolo sociale specifico; l'impatto della valutazione è potenzialmente onnicomprensivo, e non limitato a un settore; prende di mira anche azioni moralmente e professionalmente non desiderabili, anche se non illecite, senza distinzione netta tra diritto e morale.

gia si evolvano da sole[26]; in diversi ordinamenti sud-orientali, vi è un *favor* della popolazione nei confronti dei sistemi di *social credit scoring*[27].

Ma, al tempo stesso, non sono infrequenti i casi in cui si sospetta che si faccia un uso dei dati pubblici per fini discriminatori[28].

4. *La "cittadinanza a punti" nell'esperienza italiana*

Si è discusso di *social credit scoring* nell'ordinamento italiano a seguito dell'intervento dell'Autorità Garante dei Dati Personali, che ha esaminato tre casi distinti[29].

Una prima istruttoria ha riguardato il «Progetto Pollicino», indagine statistica a carattere sperimentale, promossa dalla Fondazione per lo sviluppo sostenibile, dal Ministero della transizione ecologica e dal Ministero delle infrastrutture e della mobilità sostenibili, con la quale il cittadino veniva invitato a condividere i propri dati «in forma anonima» per consentire analisi della mobilità[30] del comune di Bologna. Al termine dell'indagine, era previsto che il cittadino ricevesse premi offerti da *partner* privati.

Altra istruttoria ha riguardato l'iniziativa *smart citizen wallet*, sempre del Comune di Bologna, presentata al pubblico come la «patente digitale del cittadino virtuoso», alla quale i cittadini avrebbero potuto aderire su

[26] T. Frey aggiunge che la maggior parte delle persone tende ad essere motivata da classifiche personalizzate ed obiettive; un sistema universale, che punisce e premia, potrebbe perciò migliorare il mondo.

[27] W. Rabe - G. Kostka, *Perceptions of social credit systems in Southeast Asia: An external technology acceptance model*, *Global Policy*, 2024 hanno osservato come i cittadini di Thailandia, Indonesia, Malesia e Filippine abbiano mostrato alti livelli di accettazione nei confronti dell'implementazione ancora ipotetica del SCS, correlati con la percezione che la Cina offra opportunità economiche, mentre le preoccupazioni sulle minacce alla sicurezza non tradizionali non diminuiscono significativamente gli atteggiamenti positivi. L'atteggiamento favorevole riguarda in particolare i cittadini più giovani.

[28] A mero titolo esemplificativo, alcuni procuratori generali repubblicani hanno scritto un promemoria a Brian T. Moynihan, presidente del consiglio di amministrazione e CEO di Bank of America (BOA), osservando che l'istituto "sembra condizionare l'accesso ai suoi servizi ai clienti che hanno le opinioni religiose o politiche preferite dalla banca", a seguito della notizia di *partnership* del BOA con il *Federal Bureau of Investigations* e il Tesoro degli Stati Uniti: https://www.telegraph.co.uk/us/comment/2024/05/28/donald-trump-chinese-social-credit-debanking-us-politics/

[29] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9778361

[30] osservatoriosharingmobility.it/pollicino/.

base volontaria e che avrebbe consentito di accumulare «crediti» con l'adozione di azioni virtuose (ricorso alla raccolta differenziata e ai mezzi di trasporto pubblici, gestione oculata dell'energia, uso attivo della carta cultura, assenza di violazioni del codice stradale), da convertire in premi/incentivi messi a disposizione dal Comune e da *partner* accreditati[31].

La terza istruttoria ha riguardato il Comune di Fidenza, che ha tentato di introdurre, con proprio regolamento, la «carta dell'assegnatario» degli alloggi di edilizia residenziale pubblica, un meccanismo di *scoring* associato al comportamento tenuto dagli assegnatari degli alloggi, finalizzato al riconoscimento di benefici e sanzioni, inclusa la risoluzione e/o la decadenza del contratto di locazione[32].

Il Garante ha ribadito la necessità che queste iniziative siano sempre e comunque anticipate da puntuali valutazioni di impatto e rispettino i principi fondamentali del Regolamento UE GDPR sulla protezione dei dati personali (al momento della pronuncia non era ancora stato approvato il Regolamento sull'Intelligenza Artificiale).

Si è ricordato[33] in dottrina come il Considerando 43 del GDPR sconsigli espressamente di adottare il consenso come base giuridica nel caso in cui il trattamento sia effettuato da autorità pubbliche[34].

[31] A. Capoluongo, *"Social scoring" e "Smart Citizen Wallet" tra Cina ed Europa*, www.cyberlaws.it/2022/social-scoring-smart-citizen-wallet/.

[32] «con possibili conseguenze pregiudizievoli in capo a categorie di soggetti vulnerabili», sostiene il Garante. La delibera è del 17 febbraio 2022. Si legge «Articolo 8 (Carta dell'assegnatario) Dalla data di entrata in vigore del presente nuovo Regolamento, ad ogni assegnatario, è attribuita una carta denominata "Carta dell'assegnatario" riportante un credito espresso da un punteggio pari a punti 50. L'assegnatario è responsabile per i comportamenti violativi commessi da tutti i componenti il nucleo familiare avente diritto e da eventuali ospiti temporanei. In caso di irrogazione di una sanzione, il credito sarà decurtato dall'ammontare dei punti indicati per ogni violazione, come previsto dalla Tabella A, in calce al presente Regolamento. L'esaurimento del credito comporterà la risoluzione del contratto di locazione (e/o la decadenza ai sensi dell'art. 30 co. 1 lettera b per aver violato gravemente le norme del Regolamento d'uso) ai sensi delle disposizioni contenute nell'art. 31 della Legge regionale 8 agosto 2001 n. 24 e ss.mm.ii. Agli assegnatari che per un periodo consecutivo di tre anni, non incorrono in sanzioni, è attribuito automaticamente un incremento di punti 5, fino al raggiungimento del punteggio massimo di punti 65, o a recupero dei punti eventualmente decurtati per comportamenti sanzionati. Agli assegnatari che attivano meccanismi riparatori alternativi al precedente co. 5 è attribuito un incremento di punti 5, fino al raggiungimento del punteggio massimo di punti 65. È facoltà del Comune riconoscere ulteriori punti agli assegnatari che attivano comportamenti virtuosi nell'ambito di specifici progetti in favore della comunità condominiale».

[33] A. Capoluongo, *"Social scoring"*, *cit*.

[34] Osserva nelle Linee guida sul consenso il Gruppo di lavoro Articolo 29 che Il

Relativamente a questi casi non vi sono state altre informazioni provenienti dalle autorità o dai *media*, e non risulta sia stato dato seguito a questi progetti.

Nel primo caso si è in presenza di incentivi a fornire informazioni, il potere di controllo è penetrante, anche se non c'è graduazione dei benefici sulla base del comportamento; anche nel secondo caso vi sono incentivi a fornire informazioni, con un programma di promozione di buone pratiche e l'esercizio del potere presenta un alto tasso di discrezionalità[35]; nel terzo caso si mira alla conformazione dei comportamenti, vi è la previsione di sorveglianza e sanzioni, con il problema dell'eventuale risoluzione del contratto, e il potere è esercitato nei confronti di soggetti bisognosi, sottoponendo a condizione il godimento di un diritto sociale. Tuttavia, almeno in questi casi non si tratta di ipotesi di profilazione generale onnicomprensiva, ma di profilazioni settoriali.

5. *La piattaforma di reputazione sociale nell'esperienza italiana*

Già nel 2016 il Garante è intervenuto nei confronti di alcune società intenzionate a realizzare una piattaforma *web* (con annesso archivio informatico) per l'elaborazione di profili reputazionali concernenti persone fisiche e giuridiche, utile per rapporti commerciali[36]. La vicenda, sebbene quindi abbia avuto origine prima dei casi citati di cittadinanza a punti, ha solo di recente visto una possibile soluzione.

L'operazione, nelle dichiarazioni degli ideatori, mira a contrastare la creazione di profili reputazionali "inveritieri" e a calcolare in maniera

considerando 43 indica chiaramente che è improbabile che le autorità pubbliche possano basarsi sul consenso per effettuare il trattamento, poiché quando il titolare del trattamento è un'autorità pubblica sussiste spesso un evidente squilibrio di potere nella relazione tra il titolare del trattamento e l'interessato. In molti di questi casi è inoltre evidente che l'interessato non dispone di alternative realistiche all'accettazione (dei termini) del trattamento. Esistono altre basi legittime, in linea di principio più appropriate, per il trattamento da parte delle autorità pubbliche.

[35] E. Brivio: "l'intento di osservare i comportamenti dei cittadini per valutarne una virtuosità numericamente espressa in punti e spendibile in premi appare realmente rivolta ad applicare uno scrutinio pubblico dall'altissimo contenuto discrezionale. Né una base giuridica sufficiente può essere il solo consenso dell'interessato, sia perché anche in questo caso gli strumenti premiali possono agire in modo distorsivo, sia perché la natura pubblica dell'amministrazione comunale pone il cittadino in una situazione di squilibrio di potere"

[36] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5796783

"accurata e imparziale" il *rating* dei soggetti censiti per permettere a terzi di verificarne la credibilità, consentendo agli iscritti di documentare la posizione propria o altrui, con l'obiettivo di "incrementare il livello di fiducia" e "incentivare l'adozione di comportamenti virtuosi". Il sistema consentirebbe così una «rappresentazione tendenzialmente completa dei soggetti censiti perché riferito a tutti gli aspetti (a 360°) che concorrono a definire la loro reputazione»: viene assegnato sia un *rating* complessivo dell'affidabilità del soggetto, sia *rating* specifici ("penale", "fiscale", "civile", "lavoro e impegno civile" e "studi e formazione"), con informazioni relative anche al profilo etico dei soggetti coinvolti.

La piattaforma si basa sul caricamento volontario di documenti di ogni tipo da parte degli utenti[37], potendo riguardare anche terzi non iscritti, attraverso documenti liberamente utilizzabili come le sentenze, in questo ultimo caso senza determinazione di *rating*. Il punteggio è reso disponibile a tutti gli altri utenti della piattaforma[38].

L'Autorità ha dubitato del fondamento normativo dell'attività[39], e ravvisato violazione della tutela dei dati personali, in particolare in ordine al consenso[40] e al trattamento dei dati[41]. Con riferimento in particolare al

[37] Tra i documenti anche certificati del casellario giudiziale; certificati di regolarità fiscale; certificati relativi ad abilitazioni; diplomi; denunce; querele; provvedimenti giudiziari; ecc., provenienti esclusivamente da fonti diverse dagli interessati, non essendo ammessa la autocertificazione, comprensivi anche di documenti relativi alla sfera morale, come certificati di riconoscimento al valor civile; partecipazione ad attività di volontariato, encomi, premi, referenze, ecc. e professionali (successi e insuccessi), "articoli stampa, radio/TV".

[38] Era previsto un controllo generalizzato e diffuso sui dati attraverso il vaglio dei documenti da parte di consulenti e degli utenti; inoltre veniva previsto un "Comitato di Controllo" di vigilanza sui consulenti reputazionali.

[39] L'Autorità ha anche criticato la pretesa di rinvenire un fondamento normativo nella banca dati. Ha infatti osservato che altri sistemi di "accreditamento" derivano da previsioni di legge che ne individuano espressamente le principali caratteristiche (ad esempio, il "rating di legalità", ovvero il "rating di impresa" di cui all´art. 83, comma 10 del d.lgs. n. 50/2016), laddove i riferimenti normativi del caso in esame apparivano generici e, comunque, inidonei a giustificare la costituzione della banca dati.

[40] Il funzionamento del sistema si basa su modalità di raccolta (massiva) di dati e documenti non in linea con l'art. 3 del Codice (secondo cui i sistemi informativi e i programmi informatici vanno configurati in modo da ridurre al minimo l'utilizzo di dati personali e identificativi degli interessati).

[41] Il trattamento riguarderebbe un numero potenzialmente molto elevato di soggetti, con attendibili significative ripercussioni per i diritti individuali degli interessati in caso di violazione delle misure di sicurezza, di accessi non autorizzati o di utilizzo abusivo delle informazioni. Dacché appaiono sproporzionate anche le modalità con cui si è stabilito di

consenso, ha ricordato che esso deve essere manifestato liberamente[42], il che non avviene nel caso di necessità di contrastare gli effetti negativi derivanti da eventuali valutazioni avverse[43].

Le maggiori perplessità del Garante derivano dalla circostanza che il sistema si basa sulla raccolta di dati personali in grado di incidere significativamente sulla rappresentazione economica e sociale di un'ampia platea di soggetti, con possibili considerevoli ripercussioni sulla vita (anche privata) degli individui, influenzandone scelte, prospettive e l'ammissione a prestazioni, servizi o benefici: la "reputazione" che si vorrebbe misurare risulta intimamente connessa con la dignità[44].

Inoltre, il Garante osserva che lo strumento non può essere definito affidabile, a causa dell'assenza di riconosciuti criteri, a livello nazionale o internazionale, sulla base dei quali poter "misurare" la reputazione degli individui in modo realmente oggettivo, affidabile e imparziale, nonché della possibilità che la reputazione possa discendere da atti viziati da falsità ideologica, o da alterazioni materiali, o sulla base di impulsi delatori. Segnala poi il tema dell'opportunità di rimettere a un sistema automatizzato aspetti connessi alla reputazione.

La vicenda, commentata dalla dottrina, ha avuto un seguito, derivante dall'impugnazione del provvedimento del Garante innanzi al Tribunale di Roma: con sentenza n. 5715/2018 è stato annullato il provvedimento del Garante, in quanto si è osservato che, anche in assenza di una disciplina del *rating* «*non può negarsi all'autonomia privata la facoltà di orga-*

dare libero e indiscriminato accesso a tutti i numerosi documenti presenti sulla piattaforma, considerati i rischi che corrono gli interessati in relazione al loro successivo riutilizzo per finalità non necessariamente lecite (si pensi, ad esempio, al riuso dei dati per finalità di indagine su fatti non attinenti alla valutazione dell´attitudine professionale di candidati e lavoratori, potenzialmente confliggente con l´art. 8 della legge n. 300/1970, richiamato dall´art. 113 del Codice). Le misure di sicurezza sarebbero inadeguate, così come le disposizioni relative alla conservazione dei dati e all'informativa da rendere agli interessati.

[42] Art. 23 del Codice.

[43] Sul punto viene citato il "Parere 15/2011 sulla definizione di consenso" adottato dal Gruppo di lavoro articolo 29 per la protezione dei dati in data 13 luglio 2011, WP 187, secondo cui il consenso non può essere considerato libero se le conseguenze dello stesso "minano la libertà di scelta dell´individuo".

[44] La rilevanza e pertinenza di detti dati e documenti (parte dei quali, peraltro, in grado di rivelare aspetti anche molto delicati della vita privata delle persone) appare in taluni casi dubbia e, comunque, indimostrata. Non solo in ragione dei criteri (discrezionali) individuati come basi per il calcolo del *rating* reputazionale, ma anche per l'assenza di circostanziati elementi in grado di comprovare, empiricamente, l'effettiva incidenza di talune dinamiche etico-comportamentali sull´"affidabilità" dei soggetti censiti.

nizzare sistemi di accreditamento di soggetti, fornendo servizi in senso lato 'valutativi', in vista del loro ingresso nel mercato, per la conclusione di contratti e per la gestione di rapporti economici», e ha considerato il trattamento lecito, in quanto «*le attività di caricamento delle informazioni e di validazione e certificazione dei documenti sono soggette al consenso dell'interessato e alla volontarietà della sua azione*». Ha però confermato il divieto di trattare dati di soggetti non iscritti alla piattaforma, anche se provenienti da documenti di libero accesso.

Superata quindi la questione legata alla liceità del trattamento, la questione è stata affrontata dalla Corte di Cassazione la quale, con sentenza 14381/2021, ha accolto il ricorso del Garante e affermato che il consenso non è consapevole e quindi non può essere validamente prestato se lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili[45]. In questo senso, il punto rilevante diventa la

[45] «*in tema di trattamento di dati personali, il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento a un trattamento chiaramente individuato; ne segue che nel caso di una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali di singole persone fisiche o giuridiche, incentrata su un sistema di calcolo con alla base un algoritmo finalizzato a stabilire i punteggi di affidabilità, il requisito di consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati*». Il Garante nel maggio del 2022 si è occupato di un caso simile, in quanto elaborato sulla base di algoritmi dalla medesima piattaforma società, mediante una richiesta di informazioni all'Associazione Crop News Onlus (Cronache reputazionali oggettive personalizzate), operante nel settore del rating "reputazionale". Secondo notizie di stampa l'Associazione avrebbe promosso il Progetto Virtute 4 Students per sperimentare, nei confronti degli studenti di una scuola secondaria superiore, il rating "reputazionale". Il Garante è intervenuto in quanto il progetto si rivolgeva a studenti minori, soggetti vulnerabili. La richiesta mirava a conoscere funzionamento della piattaforma e della banca dati per valutare l'impatto dell'uso degli algoritmi, gli effetti, le misure di tutela. Sulla questione non è stato possibile conoscere gli ulteriori sviluppi, se non attraverso l'articolo di G. Cerrina Feroni, cit., la quale riferisce che «*L'Associazione ha dichiarato che il fine dell'iniziativa fosse quello di stimolare gli studenti a costruirsi una reputazione reale che coincidesse con la reputazione virtuale attraverso il proprio rating reputazionale digitalizzato per promuovere un modello economico comportamentale trasparente. Virtute calcola le singole reputazioni pubblicate dal periodico online Crop News, promuovendo quindi comportamenti legali fondati sul timore di comparire sulla testata. La riduzione di illeciti e inadempimenti contrattuali garantirebbe sia gli operatori economici, che consumatori e utenti, ma in ragione del "ricatto" morale di un rating reputazionale automatizzato, che peraltro attribuisce compensi variabili in relazione al contributo fornito da ciascuno per qualificare la reputazione documentata e tracciabile propria e delle controparti nei rapporti obbligatori. Sulla base delle informazioni fornite e di ulteriori indagini, l'Autorità ha ritenuto il trattamento illecito, in violazione delle garanzie obbligatorie dell'art. 22 del GDPR e,*

libertà del consenso[46], viziato dall'ignoranza e dall'incomprensibilità dell'operato della piattaforma.

Sulla linea della pronuncia della Cassazione, la successiva sentenza del 22 giugno 2022, n. 9995 del Tribunale di Roma ha respinto il ricorso dell'associazione, in quanto il regolamento del sistema, reso disponibile, non esplicita lo schema esecutivo dell'algoritmo, ma fornisce solo un elenco dei fattori presi in considerazione per il *rating* delle varie categorie, senza precisare come questi dati vengano poi elaborati dall'algoritmo.

L'ultima pronuncia è l'ordinanza della Cassazione n. 4327, del 10 ottobre 2023, con cui la Corte ha ritenuto che i parametri di riferimento necessari per la conoscenza e la comprensione dell'algoritmo fossero tutti contenuti nel regolamento e che quindi il consenso potesse essere espresso liberamente[47].

In tal modo, seppure con i limiti indicati nel corso della vicenda processuale (come ad esempio nei confronti dei terzi), il sistema è stato so-

soprattutto, contrario ai principi di liceità (poiché effettuato in assenza di una base giuridica sufficiente), correttezza (poiché in grado d'ingenerare discriminazioni e pregiudizi irragionevoli e sproporzionati), trasparenza (in quanto effettuato in assenza di un'informativa adeguata), minimizzazione (trattando quantità di dati indeterminate ed indeterminabili a priori), limitazione (poiché produce nuovi dati da potersi trattare per il perseguimento di finalità diverse e non necessariamente lecite), e limitazione della conservazione (affidando i dati ad una testata online). Crop News è stata quindi ammonita, mentre si è aperta una nuova istruttoria nei confronti di Mevaluate, collettore di tutti i dati raccolti.»

[46] L'art. 4 par. 11 del GDPR prescrive che il consenso sia una «manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato». In questo senso il consenso non è libero se l'interessato non dispone di una scelta effettiva, si sente obbligato ad acconsentire o subirà conseguenze negative se non acconsente (Gruppo di lavoro Articolo 29, Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, 2018, § 3.1). Se il consenso è parte non negoziabile delle condizioni generali di contratto/servizio, si presume che non sia stato prestato liberamente.

[47] Osserva la Corte che, nella vicenda, «*ad integrare i presupposti del "libero e specifico" consenso, affinché esso sia legittimo e valido, è richiesto che l'aspirante associato sia in grado di conoscere l'algoritmo, inteso come procedimento affidabile per ottenere un certo risultato o risolvere un certo problema, che venga descritto all'utente in modo non ambiguo ed in maniera dettagliata, come capace di condurre al risultato in un tempo finito. Che, poi, il procedimento, come spiegato con i termini della lingua comune, sia altresì idoneo ad essere tradotto in linguaggio matematico è tanto necessario e certo, quanto irrilevante: ed invero, non è richiesto né che tale linguaggio matematico sia osteso agli utenti, né, tanto meno, che essi lo comprendano. Ciò che rileva, invece, è che sia possibile tradurre in linguaggio matematico/informatico i dati di partenza, cosicché il tutto divenga opportunamente comprensibile alla macchina, grazie ai soggetti esperti programmatori, secondo le sequenze e le istruzioni tratte dai dati "in chiaro", come descritti nel regolamento più volte citato*».

stanzialmente ritenuto legittimo, e le perplessità sono state fugate dai giudici, richiamandosi alla trasparenza.

6. *L'automazione del calcolo del* rating

Già sulla base della direttiva 95/46/CE, la legge sui dati personali 675 del 1996, all'art. 17, stabiliva che una valutazione ad opera di un atto amministrativo del comportamento umano non potesse essere fondata unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato[48]. Sebbene quindi l'idea di proteggere la persona dalla costruzione della personalità attraverso trattamenti automatizzati sia stata presente sin dal 1995, è tuttavia solo con il GDPR che si è provveduto a disciplinare espressamente la profilazione reputazionale[49].

Si è disposto (cons. 71 e art. 22) che l'interessato ha il diritto di non essere sottoposto a una decisione che valuti aspetti personali basata unicamente su un trattamento automatizzato se non in presenza di garanzie, quali i diritti ad esserne informato, ad ottenere l'intervento umano, al contraddittorio, ad una spiegazione della decisione, alla contestazione[50].

[48] Art. 17, primo comma, l. 31 dicembre 1996, n. 675 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali).

[49] Il Considerando 24 GDPR tratta della profilazione e di come sia sottoposto il trattamento dei dati al regolamento quando riferito al monitoraggio dei comportamenti, e afferma che «per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su *internet*, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali». L'articolo 4 collega la profilazione alle valutazioni delle decisioni relative agli individui, sulla base di dati personali: «la "profilazione" (…) consiste in qualsiasi forma di trattamento automatizzato di dati personali che valuti gli aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti quali le prestazioni lavorative dell'interessato, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, la posizione geografica o gli spostamenti, laddove ciò produca effetti giuridici che lo o la riguardano o che influiscono in modo significativo su di lui o su di lei».

[50] Il Considerando 71 GDPR osserva poi che «l'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito onli-

Sul punto rilevante è la sentenza cd. *Schufa Holding* del 7 dicembre 2023 della Corte di Giustizia (C-634/21), relativa a una cittadina tedesca, alla quale era stata rifiutato un mutuo a causa del punteggio negativo (relativo alla capacità di ripagare debiti) assegnatole da una società privata di *rating*; la ricorrente aveva chiesto e non ottenuto l'accesso ex art. 15 del GDPR, ricevendo solo una spiegazione parziale degli elementi che avevano portato alla decisione, senza esplicitazione dei singoli fattori considerati e della loro rilevanza specifica ai fini della valutazione effettuata, anche perché la società considerava i propri metodi di calcolo protetti da segreto commerciale[51].

La Corte di Giustizia, in sede di rinvio pregiudiziale, ha affermato che l'attribuzione dello *scoring* può essere considerato un processo decisionale integralmente automatizzato ai sensi dell'art. 22 GDPR, in quanto si tratta di profilazione dell'interessato in grado di incidere significativamente sulla sua persona[52].

ne o pratiche di assunzione elettronica senza interventi umani. […] In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore». L'art. 22: 1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. 2. Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato. 3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione».

[51] Art. 15: «1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: (…) *h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione* di cui all'articolo 22, paragrafi 1 e 4, *e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*».

[52] «Il calcolo automatizzato, da parte di una società che fornisce informazioni commerciali, di un tasso di probabilità basato su dati personali relativi a una persona e riguardanti la capacità di quest'ultima di onorare in futuro gli impegni di pagamento costituisce un «processo decisionale automatizzato relativo alle persone fisiche», ai sensi di tale disposizione, qualora da tale tasso di probabilità dipenda in modo decisivo la stipula, l'ese-

Da ciò discendono diversi obblighi per il titolare del trattamento: utilizzare procedure matematiche-statistiche appropriate per la profilazione, mettere in atto misure tecniche e organizzative per rettificare i fattori che comportano inesattezze dei dati, minimizzare il rischio di errori e garantire la sicurezza dei dati personali, in particolare per impedire effetti discriminatori. *Tali misure comprendono inoltre quantomeno il diritto dell'interessato di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione adottata nei suoi confronti* (66).

Il dovere di motivare sul punto ha come effetto indiretto che l'erogazione del credito non potrà essere decisa che sulla base di dati pertinenti, quali inadempienze o insolvenze.

I casi citati negli ultimi due paragrafi pongono all'attenzione il tema della trasparenza in ordine al funzionamento degli algoritmi di *scoring*: esso non richiede una trattazione differente rispetto a come viene affrontato in senso più ampio, e quindi per un verso bisogna tenere conto dell'eventuale protezione dei brevetti e dei segreti commerciali, richiamata anche come antidoto all'eventuale elusione del sistema, per un verso pone un problema di conoscibilità/comprensibilità dell'operato degli algoritmi[53].

7. *La disciplina sull'IA*

Il Regolamento sull'IA[54] ha deciso di proibire, all'art. 5 i c.d. sistemi di *social credit scoring*, in particolare *l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti: i)*

cuzione o la cessazione di un rapporto contrattuale con tale persona da parte di un terzo, al quale è comunicato tale tasso di probabilità» (71).

[53] Sul punto la letteratura è oramai sterminata: ci si permette di richiamare F. Costantino, *Algoritmi, intelligenza artificiale e giudice amministrativo*, *Giurisprudenza Italiana*, 2022.

[54] Il quale mira a conciliare la tutela dei diritti fondamentali e dei valori dell'UE con l'innovazione tecnologica e classifica i sistemi di IA a seconda del rischio dell'utilizzo per la salute e la sicurezza o per i diritti fondamentali delle persone fisiche, che può essere inaccettabile, alto o basso. Viene così definito un quadro giuridico uniforme per tutti gli Stati membri.

un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità. Nella distinzione tra sistemi di IA a seconda del rischio, questi in oggetto sono classificati come a rischio inaccettabile.

Nella prima versione, il testo vietava i punteggi reputazionali solo nelle ipotesi in cui fossero adottati da un'autorità pubblica, con effetti pregiudizievoli in un contesto scollegato da quello della profilazione, o sproporzionati rispetto alla condotta, e comunque, come d'altronde anche nell'attuale versione, non vietava le ipotesi in cui i sistemi di *scoring* si limitassero ad attribuire situazioni di vantaggio.

Il Considerando 17 afferma che «*I sistemi di AI che forniscono un punteggio sociale delle persone fisiche per finalità generali possono portare a risultati discriminatori e all'esclusione di determinati gruppi*» e, senza fare riferimento alle sole autorità pubbliche (come nella versione in bozza), afferma che i punteggi «*ledono il diritto alla dignità e alla non discriminazione e i valori di uguaglianza e giustizia*» (la precedente formulazione preferiva un più dubitativo "possono ledere").

La disciplina appare evidentemente fare riferimento al Sistema di Credito Sociale cinese.

Il Regolamento ha scelto di fornire una disciplina minima, senza regolare le ipotesi di profilazione tesa ad attribuire solo vantaggi o premi, il che avrebbe comportato il rischio di intervenire sulle operazioni commerciali che offrono sconti e promozioni.

Si può quindi dubitare che, nei casi italiani, in cui i premi sono stati proposti per settori diversi da quelli per cui sono stati raccolti i dati, si rientri nella fattispecie delineata dall'art. 5. Inoltre, l'eventuale decisione volontaria di partecipare a queste iniziative invece di mettere al riparo queste ipotesi da profili di illegittimità sembra aggravarle, in quanto i cittadini che non vi aderiscono automaticamente siano considerati potenzialmente meno virtuosi, o comunque meno inclini a una buona condotta civica.

Il Regolamento si occupa anche di altri sistemi di credito: il considerando 58 stabilisce che «*È inoltre opportuno classificare i sistemi di IA utilizzati per valutare il merito di credito o l'affidabilità creditizia delle persone fisiche come sistemi di IA ad alto rischio, in quanto determinano l'accesso di tali persone alle risorse finanziarie o a servizi essenziali quali l'alloggio, l'elettricità e i servizi di telecomunicazione. I sistemi di IA utilizzati*

a tali fini possono portare alla discriminazione fra persone o gruppi e possono perpetuare modelli storici di discriminazione, come quella basata sull'origine razziale o etnica, sul genere, sulle disabilità, sull'età o sull'orientamento sessuale, o possono dar vita a nuove forme di impatti discriminatori». Esso fa il paio con il Considerando 71 del GDPR il quale cita, come esempi di decisioni automatizzate che possono incidere sui diritti e le libertà degli individui in maniera rilevante, il rifiuto automatico di una domanda di credito *online*.

8. *Considerazioni conclusive*

Il tema del *social credit scoring* appare destinato, con la raccolta sempre più ampia di dati e il ricorso sempre più intenso a strumenti di automazione, a porsi con sempre maggiore frequenza.

Del resto, appare allettante, per soggetti pubblici e privati, la prospettiva di incrementare il livello di fiducia nella società e di incentivare l'adozione di comportamenti virtuosi, prospettata con formulazione simile sia nel caso cinese (§2) che in quello italiano (§5).

Serviranno ulteriori riflessioni e interventi regolatori, oltre che analisi caso per caso, per distinguere tra casi di *scoring* leciti e casi di *scoring* illeciti.

Certamente diventa sempre più facile e interessante immettere, per le valutazioni e le predizioni, elementi ulteriori, più o meno connessi a quelli relativi ai comportamenti e alle prestazioni eseguite in un determinato settore (e in molti casi potrebbe essere complicato capire se questi elementi vadano considerati spuri, v. §5).

Per un verso, la promessa di trasparenza per la conoscenza dei dati e degli algoritmi (§6) dovrebbe consentire di identificare i possibili elementi spuri e di sindacare la correttezza della misurazione del punteggio reputazionale.

Oltre a questa garanzia, la previsione di intervento umano e la corretta programmazione delle dotazioni informatiche appaiono imprescindibili.

La giurisprudenza sinora sembra ancora dare fin troppo rilievo al consenso (§5), che appare illusorio di fronte a sistemi che mirano a coinvolgere categorie intere di soggetti (per cui la decisione di non partecipare potrebbe essere fonte di pregiudizi (§5)), o che propongono premi ed incentivi rispetto ai quali la profilazione può non essere percepita come problematica (§4). Le autorità e la stessa giurisprudenza devono acquisi-

re la capacità di cogliere i possibili pregiudizi (§5), anche in questi ultimi casi, e potrebbero essere chiamate anche ad effettuare degli sforzi interpretativi, rispetto alla lettera del Regolamento (§7): del resto, è stato notato come proprio la formazione e il ricorso a liste rosse siano caratterizzati da alta discrezionalità, laddove invece le liste nere difficilmente sono il frutto di scelte discrezionali, in quanto collegate a violazioni di prescrizioni normative (§2)[55].

Lo scrutinio dovrebbe essere rigoroso, quanto più l'intervento sia penetrante e possibile fonte di pregiudizi.

[55] E. di Carpegna Brivio, *Pari dignità sociale*, *cit*., 31.

Patrizio Rubechini

CYBERSECURITY PERSPECTIVES IN ITALY. PROTECTING THE NATIONAL ECONOMY THROUGH NEW TECHNOLOGIES

1. *Nature of the problem*

No public or private organisation, interest group, company, or end-user can claim immunity from cyberattacks, given the widespread access to the Internet. The spectrum of attacks includes traditional intrusions such as ransomware, which renders data unreadable and demands a ransom for decryption, and malware, encompassing all forms of malicious code designed to disrupt the target device. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks aim to incapacitate websites by overwhelming them with service requests. Other methods, such as mail bombing, seek to disrupt email management, while sophisticated techniques like spoofing, Man-in-the-Middle (MitM) and phishing present users with deceptive environments to illicitly obtain credentials and sensitive information.

The scale of the phenomenon is considerable[1]: in Italy, 42 million cybersecurity events were recorded in 2021, marking a 16% increase from the previous year. This figure rose to approximately 56 million in 2022/2023 and 69 million in 2024, years marked by heightened international tensions due to the Russian-Ukrainian conflict and the escalation of hostilities between Israel and Hamas. The global trend remains unchanged[2], where

[1] Source: Fastweb SOC, Clusit report 2022/2023/2024/2025.

[2] The Economist already reported on this in 2020: "*During the pandemic a digital crimewave has flooded the internet*", in *www.economist.com*, dated 17 August 2020.

severe attacks[3] reached 12,495 events between January 2019 and June 2024, with a notable increase from 796 attacks in January 2019 to 1,637 in June 2024, representing 13% of the total since 2019 and a 23% rise compared to the second half of 2023. Certain sectors are particularly vulnerable: in the first half of 2024, 18% of global threats targeted the healthcare sector (9% in Italy)[4], 13% targeted government, military and public order sectors (11% in Italy), 7% targeted the ICT sector (4% in Italy). When considering these sectors alongside others such as transportation, professional services, media, retail, manufacturing, energy, education, telecommunications, and finance, global cybercrime losses amounted to approximately USD 6 trillion in 2021, rising to USD 8 trillion in 2023, with projections reaching USD 10.5 trillion by 2025[5].

Therefore, the impact of cyber threats underscores the critical importance of developing and implementing cybersecurity strategies and techniques aimed at preventing, containing, and resolving malicious events, in order to safeguard interests that are both specific and general in nature. The protected interest is specific when considered within the confined context of an individual company or public administration affected by a cyber incident. However, it assumes a general – and thus more significant – dimension when such entities are responsible for managing, through computer networks and systems, services and functions that are essential to citizenship and to the proper functioning of the State apparatus as a whole.

When a cyberattack has the capacity to paralyse a production chain, disrupt the provision of utility services, or halt or impede the transportation network, a typical knock-on effect ensues, impacting users, businesses, public administrations, and, consequently, the State itself.

[3] A "severe" threat is defined as a cyber threat whose impact is proven to be widespread in different aspects of society, politics, economics and geopolitics. The alarming overall figure for cyber threats detected globally in 2024, according to Microsoft Digital Defense Report 2024 and regardless of the degree of severity attributed, is 600 million event per day.

[4] The special nature of the interests protected by the healthcare sector prompted ENISA (the European Cybersecurity Agency) to dedicate a special analysis to it, with the document titled "*Health Threat Landscape*" published in July 2023 (see *enisa.europa.eu*). From it follows that more than half of the attacks examined by the survey (215 in total, in the period January 2021 to March 2023) concerned European hospitals (mainly in France, Spain, Germany, Italy and the Netherlands) and that almost all of them were linked to ransom demands for stolen data.

[5] Source: 2023 Official Cybercrime Report (at *cybersecurityventures.com*).

Such disruptions undermine the regular and orderly operation of the State.

This is why cybersecurity must be regarded not merely as a sector, but as a complex set of measures in which technical aspects designed to counter cyber threats necessarily coexist with social, economic and legal dimensions arising from the effects of such threats.

The multi-polar nature of cybersecurity also explains why the management of cyber threats cannot be entrusted solely to the economic and organisational capacities of individual companies, even though they may implement their own defence programmes, invest in continuously updated software and employ specialised experts. Nor can the responsibility for cyber protection be placed upon end-users of the Internet or those services that are themselves the targets of such threats.

Rather, it is incumbent upon public institutions to channel and treat cybersecurity as a public good, analogous to national defence, of which it increasingly constitutes an ongoing evolution[6].

Nevertheless, in the management of cybersecurity measures it is es-

[6] On the notion of cybersecurity and its relevance as a possible public good, see R. Brighi, P.G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in *Federalismi*, 21/2021, 19 ff., according to which "*At a high level of abstraction, on the technical and organisational profile, cybersecurity is expressed in three categories of measures (or controls). Firstly, the preparation of measures to prevent the computer incident with the aim of preventing the risk from manifesting itself, controlling the vulnerability points of the system and protecting it from attacks; secondly, measures for monitoring adverse events that in the event of a security incident are aimed at detecting the harmful consequences and acting on the system to improve security; finally, recovery measures that in response to the event allow the damage to be minimised by the timely reactivation of the system and its functionalities, without any loss of data. Each area encompasses a wide range of technical tools and organisational measures: access control, disaster recovery, encryption, hardware and software for perimeter defence, intrusion detection systems and physical security measures, etc.*", but see also, 27, where "*The first direct consequence of applying the theory of public goods would require a comparison with the positive and negative externalities of the private good, cybersecurity, to which one would like to extend this treatment. The first negative externality to be analysed is the diversionary effect: some cybersecurity technologies, such as firewalls, belonging to the resilience dimension, simply divert attacks from a more impenetrable target to one that is more easily attacked, which means that improving the security of one actor may result in a lower security status for the systems* […]. *The second negative externality of cybersecurity is the externalisation of costs: when software fails to prevent an intrusion or a service provider fails to block a malware attack, there is no mechanism through which to hold these private actors responsible for the costs of these failures. The costs are borne entirely by the end user*" (translated by the author).

sential to consider the security and protection choices made by private actors – particularly by the largest companies, which, by virtue of their size or the nature of their activities, constitute central hubs in the functioning of the national system. Given that economic operators frequently represent the primary targets of cyberattacks and, consequently, the first line of defence for the system[7], the most effective approach is a multi-level one.

In this model, instruments provided by proximity actors – namely, those closest to the end-users of threatened services, such as individual businesses and administrations – serve to support and reinforce the tools developed at the central institutional level.

Accordingly, this necessitates an arrangement that draws upon the model of disaggregated organisation[8], within which not fully articulated forms of partnership are incorporated.

In practice, public and private operators communicate and cooperate with one another in pursuit of a common objective: the protection and cybersecurity of the national system.

Moreover, such a collaborative model is applicable in all instances in which the State intervenes in the economy for purposes of general interest. That is, beyond the economic policy objectives actually pursued, the State must also ensure the protection of both the substance of its intervention and the potential business developments arising therefrom. Consider, for example, cases in which the State rescues, acquires or simply participates in the capital of companies of national importance operating in sensitive or strategic sectors – such as biotechnology, security (and, in particular, cybersecurity), transport, energy, communications, or research more broadly. The patents held by such entities, or more generally the information they possess and process in the course of their activities, thereby acquire a public character derived from the underlying public

[7] This is evidenced by the fact that in the first half of 2024, 19% of the total number of cyberattacks in Italy concerned the manufacturing sector and 11% the transport/logistics sector (source: Clusit Report 2024, cited above), since these are clearly areas where private initiative is prevalent.

[8] S. Cassese, *Lo Stato ad amministrazione disaggregata*, in *Rivista trimestrale di diritto pubblico*, 2/2020, 467 ff. It should be noted how, in the Italian cybersecurity sector, the unbundled model was confirmed in 2021 with the establishment of the National Cybersecurity Agency (ACN-NCA), a public body with purely supervisory and technical functions (both instrumental and performance-related) and which, due to the issues it handles, naturally places itself within the open perimeter of a supranational collaboration network of a European matrix.

ownership of the entrepreneurial function, rather than from the entrepreneurial activity considered itself.

In other words, when the State assumes the role of entrepreneur, the sensitive information generated in this capacity must be adequately protected – not merely, or not only, out of respect for privacy regulations, but because the management of such data may have a significant impact on the country's level of protection against both external and internal threats to its functioning. These threats now operate almost exclusively via the Internet and make no distinction as to whether the "target" entity is public or private.

The objective of a cyberattack is, in fact, to create chaos, blockages or suspensions in the normal functioning of services for users. Given that such services are now provided by both public and private entities, isolated models of protection are no longer viable.

The widespread interconnection that characterises contemporary society – in which tools are provided by a multitude of private actors (such as SPID, which enables citizens to interact with public administration at all levels) or in which functions of public relevance are exercised or managed in a predominantly digital manner by private operators (such as public notaries or payment services like PagoPA) – necessitates a systemic vision. This vision must recognise information networks, and the data transmitted across them, as resources of primary importance for the regular functioning of the country, regardless of the public or private nature of the entities involved and, in any case, in light of the national interest in protecting the strategic role they play.

Accordingly, alongside the traditional approach of the entrepreneurial State – which intervenes for remedial purposes when the market fails and thus protects the object of its intervention – a more modern approach has emerged.

The digital State of the third millennium is an entity that recognises the strategic value of data and the networks through which they are transmitted and exchanged and provides dedicated protection tools that are no longer limited to reactive interventions following adverse events. Instead, the prevailing attitude is one of prevention, through proactive measures adopted in the interest of the proper functioning of the "country system", which now presents itself as a predominantly networked environment, or at the very least, as one in which services are primarily and preferably accessed online[9].

[9] Law 124/2015 or the so called Madia Reform introduced the "digital first" model into Italian legal system (but the concept was also taken up and updated in the 2022-2024

This reconstruction gives rise to several pertinent questions. How should the information upon which this system is based – often characterised by substantial volumes of digital data (commonly referred to as "data lakes") – be managed? Is there a need for a dedicated body, or an *ad hoc* structure within the remit of an existing authority, tasked with uniformly regulating the use and protection of operators' data against external and internal threats? Is there a necessity for last-resort govern-

Three-Year Plan for Information Technology, at *AGID.gov.it*), which is still valid in the relationship between users and the public administration and, above all, at the organisational level of the latter, understood no longer as a fragmented and "watertight compartmentalised" entity – at least this was the intention – but as a complex entity capable of profitably using technology in the pursuit of institutional purposes (see B. Carotti, *L'amministrazione digitale: le sfide culturali e politiche del nuovo Codice*, in *Giornale di diritto amministrativo*, 1/2017, 7 ff., who frames the argument in terms of the "redefinition" of processes). On the other hand, the uncomfortable criticality represented by the territorial and educational digital divide that plagues Italy cannot be ignored here. On this point, see the contributions by F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità*, *Il diritto dell'informazione e dell'informatica*, 2/2015, 261 ff. (where the digital divide is also analysed as a possible counter-limit to the digitisation processes "imposed" by the rules); G. Sgueo, *I servizi pubblici digitali*, in V. Bontempi (ed.), *Lo Stato digitale nel Piano nazionale di ripresa e resilienza*, Rome, Roma TrE-Press, 2022, 119 ff., in which, in the face of some progress, the persistence of a series of digital delays in the country and among the population is noted ("*The Italian score in the DESI, regarding the state of digitalisation of public services, placed Italy in 19th position in 2020. In 2021, Italy gained one position, rising to 18th place. The figure reveals some positive aspects. These include, in particular, the high number of digital identities and the increase in the number of people using e-government services, which rose from 30% to 36%. However, it is far from the EU average of 64%. Nevertheless, there is still room for improvement. Especially with regard to the still low level of innovation in the actions of public administrations, poor online interactions between administrations and users, as well as gaps in digital skills and training of public employees. According to the 2020 ISTAT surveys, of the 36% of the active population that interacts online with the PA, 29% do so mainly by downloading forms from public administration websites (in 2019 it was 21%). 27% (up from 24% in 2019) by searching for information on PA websites; 21% (up from 18% in 2019) instead of sending documentation*", translated by the author); G. Melis, *L'amara denuncia di Renato Spaventa nel 1928: "leggi e decreti non bastano se non c'è la volontà di applicarli"*, in Osservatorio Stato digitale dated 31/12/2022, at *irpa.eu*, with reference to the ancient origin of training gaps in the public sector. For a critical analysis on the subject, see S. Cassese, *Amministrare la nazione. La crisi della burocrazia e i suoi rimedi*, Milan, Mondadori, 2023; G. Sgueo, *Reclutamento e formazione del personale*, in V. Bontempi (ed.), *Lo Stato digitale nel Piano nazionale di ripresa e resilienza*, cited above, 23 ff. For an in-depth study on the causes of Italy's digital backwardness, see G. Sgueo, *Il piano per la formazione delle competenze digitali e il programma "repubblica digitale"*, in V. Bontempi (ed.), *Lo Stato digitale nel Piano nazionale di ripresa e resilienza*, cited above, 29 ff.

ance instruments capable of vetoing the use of such information where it diverges from, or otherwise deviates from, the shared policies of the State? Furthermore, has the COVID-19 pandemic influenced, and if so in what manner, the demand for protection of information assets attributable to the national system?

In seeking to address these questions, the initial approach must necessarily begin with a definition – specifically, the European one. The term "cybersecurity" is defined as "*the set of activities necessary to protect network and information systems, the users of those systems, and other persons affected by cyber threats*," as set forth in Article 2 of EU Regulation 2019/881, the so called "Cybersecurity Act". Through this regulatory initiative, the European Union sought to consolidate the operational support role provided to Member States by ENISA (the European Union Agency for Cybersecurity) and to lay the foundations for the establishment of a common cybersecurity certification framework for information and communication technologies. Consequently, we observe the stabilisation of a supranational regulatory model that encompasses all measures and procedures operating in the domains of prevention, detection, and management of cybersecurity breaches.

In Italy, however, the concept of cybersecurity – while the European definition has been transposed into domestic law through Legislative Decree No. 123/2022 – is further enriched with additional nuances. The Italian approach more fully incorporates the objectives of existing sectoral legislation, framing cybersecurity as "*the set of activities* […] *necessary to protect networks, information systems, computer services, and electronic communications from cyber threats, ensuring their availability, confidentiality, and integrity, and guaranteeing their resilience, also for the purpose of protecting national security and the national interest in cyberspace*" (Article 1, paragraph 1, letter a), Law Decree No. 82/2021)[10]. These developments, among others, have seen a marked increase in the context of the aforementioned international tensions and, in particular, as a result of the pandemic and the consequent surge in the use of digital connectivity services[11]. According to the Cybersecurity & Data Protec-

[10] Decree Law No. 82/2021 on "*Urgent provisions on cybersecurity, definition of the national cybersecurity architecture and establishment of the National Cybersecurity Agency*" was subsequently converted with amendments by Law No. 109 of 4 August 2021.

[11] The origin of this increase is to be found in the use of tools such as "smart working", "remote working", DAD – distance learning, but also more simply in the greater use of online technology for purchases and booking/use of services, e.g. due to the lockdown

tion 2022 Observatory of the School of Management at Politecnico di Milano, in the first half of 2021, 31% of large Italian companies reported an increase in cyberattacks compared to the previous year[12]. In 2022, this situation deteriorated further, primarily due to geopolitical tensions arising from the conflict between Russian and Ukrainian forces. According to the report of the National Cybercrime Centre for the Protection of Critical Infrastructures (CNAIPIC) of the Postal Police, the number of attacks detected in Italy rose by 138% – from 5,434 in 2021 to 12,947 in 2022 – targeting the country's critical and strategic infrastructures. The majority of these incidents were large-scale and demonstrative in nature, with a low rate of actual damage, but were frequently attributable to criminal groups with political links to ongoing events in the Donbass and Ukrainian regions – so called "State sponsored attacks" (SSA) – as possible responses to the international sanctions imposed by most Western countries against Russia. More recently, the phenomenon appears to have stabilised: in the first half of 2024, CNAIPIC reported a total of 5,903 attacks and 30,933 security alerts.

Accordingly, the issue of cybersecurity clearly encompasses a broad spectrum of subjects: not only businesses and institutions at all levels – which are increasingly computerised and networked – but also all individuals who, irrespective of the device they employ (be it a personal computer, smartphone, tablet, cloud service, or data storage solution), access the Internet.

Recent developments confirm this expansive scope. In early February 2023, the competent authorities in Italy – specifically the Computer Security Incident Response Team (CSIRT) established within the National Cybersecurity Agency (ACN/NCA) – identified an hacker attack of global proportions. This attack exploited widespread vulnerabilities in servers distributed across the world, resulting in the most significant disruptions in France and Finland, but also affecting Canada and the United States, with approximately 120 countries impacted overall. In Italy, several small and medium-sized enterprises, predominantly located in the

and past restrictions on movement (COVID-19 vaccine booking procedure, applications for bonuses and various economic supports e.g. those that can be requested through the INPS or Agenzia delle Entrate portal, booking of public administration services in general).

[12] Source: *som.polimi.it*, *clusit.it*. In particular, 1053 serious incidents were recorded in the first half of 2021, an increase of 15% compared to the first half of 2020, as reported by the Clusit Report 2021.

central and southern regions were affected, although no more than twenty servers were directly involved and no critical sector was compromised. Nevertheless, during the same period, major companies such as Acea (an important multi-utility provider established in Rome), Telecom and the Libero and Virgilio email platforms, experienced substantial disruptions in the management of user support information systems, which appeared to be potentially linked to the described global attack[13].

Moreover, this phenomenon now exhibits clear continuity over time. In particular, within the institutional sphere, numerous italian entities have been affected: the administrations of the Municipality of Torre del Greco (January 2023), the Municipality of Taggia (March 2023), ASL 1 of Avezzano-Sulmona-L'Aquila (May 2023), the University of Salerno and the Gestore Servizi Energetici (GSE) (July 2023). In August 2023, large-scale attacks targeted eight national credit institutions and the websites of italian public transport companies in Palermo, Siena, Bergamo, Bolzano, and Naples, as well as the Water Company and the Municipality of Palermo[14]. Further institutional victims include ASP Basilicata (January 2024), the Port Authority of the Northern Tyrrhenian Sea (March 2024), the University of Siena (May 2024), ASST Rhodense (June 2024), the Ministry of Culture (July 2024), the University of Genoa (September 2024), along with numerous other medium-sized and small private entities[15].

It is perhaps for this reason that, within IT circles, it is commonly asserted that there are two categories of recipients of cybersecurity measures: those who have already been attacked, and those who are not yet aware that they have been attacked.

2. *Measures implemented: between the EU and the nation-State*

When the State acts to protect its own strategic interests, it does so through the adoption of legal norms[16], which serve as instruments for

[13] In particular, the worldwide "down" was associated with members of the Nevada Ransomware criminal group, while the Russian-speaking cybergang called Black Basta was behind the disruptions suffered by the Acea group.

[14] Source: *cybersecurity360.com*, *ansa.com.*

[15] Source: DRM – Dashboard Ransomware Monitor.

[16] The notion of rules and regulations referred to is a broad one already introduced by the OECD ("*the diverse set of instruments by which governments set requirements in enterprises and to citizens*" (OECD, Report on Regulatory Reform, Paris, 1997). On this

managing and responding to potential threats to the protected asset. In the field of cybersecurity – understood as the discipline encompassing IT procedures designed to safeguard national networks and strategic information systems from cyber threats – the national regulatory framework is structured around three principal guidelines. The first is Legislative Decree 65/2018[17], which transposed the European Directive NIS 1 (Network and Information System Security, 2016) and which has now been substantially repealed by Legislative Decree No. 138/2024, implementing the NIS 2 Directive[18]. The second guideline consists of the so called European Cybersecurity Act, namely EU Regulation 2019/881. The third is Decree-Law No. 105/2019[19], which established the national cybersecurity perimeter. These instruments[20] – unlike previous legislative interventions, which proved largely ineffective in addressing emerging issues de-

point, see M. D'Alberti, *Riforma della regolazione e sviluppo dei mercati in Italia*, in G. Tesauro and M. D'Alberti, *Regolazione e concorrenza*, Bologna, Il Mulino, 2000, 171 ff. For a review of economic and political science theories on the notion of regulation, see A. La Spina - G. Majone, *Lo Stato regolatore*, Bologna, Il Mulino, 2000, 23 ff.

[17] Legislative Decree 65/2018 – Implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of network and information system security within the Union.

[18] The NIS 2 Directive – Network and Information System Security, in force since 27 January 2023 but whose deadline for national transposition expired on 18 October 2024, absorbs the previous NIS 1, significantly widening the number of subjects to which it is applicable and introducing the compulsory nature of a multi-risk management model of the cyber threat (the so-called "risk assessment"). On the subject of the so-called risk of the technological unknown, see the contribution of A. Barone, *Il diritto del rischio*, Giuffrè, Milano, 2006, 41 ff., for whom "[…] *the inability of science to provide 'certainties' tends to shift the jurist's reflection from the 'legal construction of science' to the 'legal construction of risk as a consequence of scientific and technological uncertainty'*" (translated by the author). While, for a broader reflection on the relationship between technological risk administration and public administration see: Id., *Amministrazione del rischio e intelligenza artificiale*, in *European Review of Digital Administration & Law – Erdal*, Vol. 1, 1-2/2020, 63 ff. The topic of risk, from the perspective of a public administration that in the application of the precautionary principle (also where arising from the introduction of new technologies) is defined as "reflexive", is also addressed in Id., *The "reflexive" Public Administration*, in Law and Society, 1/2019, 1 ff.

[19] Decree-Law 105/2019 – Urgent provisions on the perimeter of national cybersecurity and regulation of special powers in sectors of strategic importance, converted by Law No 133 of 18 November 2019.

[20] For a reconstruction of the regulatory evolution from European and national perspectives see A. Contaldo - D. Mula, *Cybersecurity Law - Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa, Pacini, 2020; L. Martino, *Cybersecurity in Italy. Governance, policies and ecosystem*, Springer, Cham, 2024.

spite the efforts undertaken[21] – are notable for having adopted a prescriptive approach towards their final recipients, at least in certain respects.

In addition, five further regulatory instruments have recently been introduced[22], which serve to update and complete – though at times complicate the future coordination with existing domestic regulations – the European and national cybersecurity framework. The first of these is the DORA Regulation (Digital Operational Resilience Act), which entered into force on 16 January 2023 and has been binding since 17 January 2025. This regulation is limited to the financial sector and aims to harmonise the cyber resilience systems of banks, insurance companies and cryptocurrency operators across the European Union. The second instrument is the CER Directive (Critical Entities Resilience, EU Directive 2022/557), transposed in Italy by Legislative Decree No. 134/2024[23]. This directive requires Member States to identify a list of critical entities – both public and private – operating in core sectors of society and the national economy [24], making them subject to both kinetic (i.e. passive) security measures designed to protect physical locations exposed to potential cyberattacks, as well as to common coordination and surveillance strategies. The third instrument is the Cyber Resilience Act (CRA), approved in October 2024 and expected to be effectively applied in 2027, which establishes minimum security standards for interconnected digital devices placed on the EU market (i.e., the Internet of Things). The fourth is the Cyber Solidarity Act (EU Regulation 2025/38), effective since 4 February 2025, which introduces a pan-European cyber-protection

[21] See the establishment of ENISA in 2004, conceived as a coordination structure with no permanent character and entirely subordinated to the competences of individual member States.

[22] The sixth regulatory intervention, at European level, is also worth-mentioning, namely Regulation EU/2023/2841 issued on 13 December 2023 that entered into force on 7 January 2024, which establishes measures for a high common level of cybersecurity in the institutions, bodies, offices and agencies of the Union (introducing a framework for the management, governance and control of cybersecurity risks that takes into account business continuity and crisis management), as a demonstration of the central role that the EU assigns to the sector.

[23] Legislative Decree 134/2024 – Implementation of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical actors and repealing Council Directive 2008/114/EC.

[24] This new framework extends its scope from the previous Directive 2008/114/EC to include core sectors such as energy, food production, banking and finance, health, water and markets, and digital infrastructures (cloud, data centres).

function – referred to as a "European shield" – based on the sharing of common mechanisms for detecting, responding to and reviewing cyber threats through mutual cooperation among various national Security Operation Centres (SOCs).

Finally, with Law No. 90/2024[25], Italy has, on the one hand, sought to anticipate the contents of the NIS 2 Directive and thereby prepare the domestic context for a general process of strengthening national cybersecurity (for example, by introducing the figure of the cybersecurity contact person in major public bodies and by defining precise reporting obligations for cyber incidents). On the other hand, it has intensified criminal penalties for offences related to the sector, such as unauthorised access to data, damage to computer systems and extortion through cyberattacks.

The operational horizon that lies ahead for all stakeholders will therefore be highly complex, as the aforementioned measures will be required to coexist with the currently applicable national and European regulations or, at the very least, to interact with their respective effects.

Specifically, the regulations presently in force include Legislative Decree No. 138/2024, which transposes the NIS 2 Directive and provides for Italy's adaptation to the common cybersecurity standards established by the European Union[26]. This decree introduces rules for the coordination and sharing of data at both the domestic and supranational levels[27] and mandates that the competent NIS authority – namely, the National Cybersecurity Agency (ACN/NCA) – identify and compile a list of so called "essential and important entities". These entities operate in key sectors or, more generally, in critical fields that are typically subject to Italian jurisdiction[28]. Irrespective of their public or private legal status,

[25] Law 90/2024 – Provisions on the strengthening of national cybersecurity and cybercrime.

[26] Through the National Cybersecurity Strategy (Art. 9, Legislative Decree 138/2024), which in turn is subject to periodic evaluation by ACN, "*strategic objectives and the resources needed to achieve them, as well as appropriate strategic and regulatory measures to achieve and maintain a high level of cybersecurity*" are identified.

[27] Internal coordination between national authorities involved in cyber protection dynamics is provided for in Article 14 of Legislative Decree 138/2024, while Article 19 outlines Italian participation in EU-CyCLONe, the network of liaison organisations for cyber crises. Article 20, on the other hand, provides for cooperative models among the national CSIRTs, which constitute computer emergency response centres in the event of a threat.

[28] Pursuant to Article 1(f), Legislative Decree No. 138/2024 provides, in fact, the "indication of the criteria for the identification of the entities to which this decree applies

and by virtue of their use of networks and information systems, they provide core services essential to the maintenance of social and economic activities that are fundamental to the nation [29]. For such entities, the legislation requires, on the one hand, the adoption of "*appropriate and proportionate technical, operational, and organisational measures* […] *to manage the risks posed to the security of the information and network systems these entities use in their activities or in the provision of their services, as well as to prevent or minimise the impact of incidents for the recipients of their services and for other services*" (Art. 24). On the other hand, they are obliged to report major incidents without delay (Art. 25). However, this regime excludes smaller operators engaged in non-sensitive sectors, specifically micro- and small enterprises with fewer than 50 employees and an annual turnover or budget not exceeding EUR 10 million.

This latter exclusion stands in contrast to the IT protection framework established for larger companies and, evidently, fails to account for the inherent transversality and diffusivity of cyberattacks, which can be equally detrimental to the stability of the national system regardless of an operator's turnover. Rather, the risk is determined by the IT modality through which certain services are delivered, the nature and content of the data potentially compromised during a malicious event and, crucially, the possibility of cascading effects arising from the interconnection and scale of digital archives[30].

The regulatory provisions outlined above clearly demonstrate the

and the definition of the relevant obligations with regard to information security risk management measures and incident reporting".

[29] Legislative Decree 138/2024, with Annexes I to IV, provides cataloguing of the economic and operational sectors deemed relevant. With NIS 2, the subjective distinction contained in the NIS 1 Directive between Operators of Essential Services - OSE and Digital Service Providers - FSD is definitely overcome, in favour of the broader categories of "essential subjects" (such as public administrations, operators in energy, healthcare, space, banking, transport, digital infrastructures, water) and "important subjects" (e.g. operators of postal and courier services, waste management, the chemical sector, the agri-food sector), also setting a size-cap beyond which the discipline becomes applicable anyway, in fact, with the aim to solve qualitatively, and not only quantitatively, the problem of the subjective extension of the measures already contained in NIS 1.

[30] Consider that, according to the results of the 2024/2025 research of the Cloud Transformation Observatory of the Politecnico di Milano School of Management, in 2024 Cloud technology will be adopted by 67% of small and medium-sized enterprises (there will be a 21% growth in 2024 for the expenditure in Public and Hybrid Cloud in this sector, with a value of EUR 581 million).

particular attention the State devotes to certain categories of sensitive or strategic services essential to its proper functioning. They also confirm that, within the current legal system, there already exist cybersecurity instruments and procedures designed to protect businesses, which are thus suitable for ensuring the protection of the public interest. This public interest is to be understood both in its immediate manifestation, as seen in the "entrepreneurial State" and in its more nuanced form, whereby the State acts as a regulator of specific sectors of the national economy[31].

At the European level, however, the applicability of the Cybersecurity Act remains significant. As the second of the three principal guidelines identified, it seeks, on the one hand, to reposition and redefine the role of ENISA (the European Network and Information Security Agency, established in 2004). On the other hand, it has the considerable merit of initiating the process for the creation of a European certification framework for cybersecurity, thereby paving the way for subsequent measures – such as the EU's DORA Regulation and Italy's Legislative Decree No. 123/2022 – as well as forthcoming instruments, notably the Cyber Resilience Act. These developments advance the regulatory landscape to a more operational phase, framed in terms of "*security by design*".

Through this regulatory instrument, the European Union has thus charted a path for the future: it has recognised the necessity of centralising European cybersecurity within a specialised agency – a process that remains ongoing, but which promises to standardise technical frameworks and related policies at the continental level. Simultaneously, it has laid the foundations for equipping ENISA and the Member States with new and robust tools for cyber protection, while also involving and empowering individual national authorities, for example, in the certification of cyber products. The establishment of a unified cybersecurity certification framework, which in Italy is supplemented by the well-known Legislative Decree No. 123/2022[32], has a direct impact on manufacturers and, consequently, on companies. Already at the design stage of individual products or services – through the principle of "security by design" – companies are, although not yet legally obliged, able to standardise requirements for the protection of user data. Furthermore, the progressive proliferation of the "*Internet of Things*" (IoT) – that is, goods and servic-

[31] On this topic, see S. Cassese (ed.), *La nuova costituzione economica*, Bari, Laterza, 2021 and, in particular, Id., *La nuova costituzione economica*, *ibidem*, 389 ff.

[32] See, *supra*, footnote 11.

es of everyday use which presuppose and are realised through network connectivity – represents the natural destination of the project outlined in the Cybersecurity Act and the soon-to-be-operational Cyber Resilience Act (December 2027).

Finally, the third principal guideline to be considered is Decree-Law No. 105/2019, which establishes the national cybersecurity perimeter at the domestic level. This legislative measure represents the Italian legislator's regulatory response to the new and urgent protection needs that have rapidly emerged in recent years in the field of network security. Notably, it addresses additional and equally significant aspects when compared to the European Cybersecurity Act (CSA), with which, moreover, it does not present any direct regulatory overlap[33]. The Cybersecurity Act (CSA) is, in fact, primarily aimed at the indirect protection of digital data through a regulatory framework directed at businesses, introducing certification mechanisms for products, services, and processes related to information and communication technologies. By contrast, Decree-Law No. 105/2019 represents a necessary completion of the work initiated by the Italian State in 2018 on this matter. Through the expansion and specification of the criteria for identifying the range of actors involved in the implementation of cybersecurity – namely, by introducing the concept of the "*National cyberSecurity Perimeter*" (PSN/NSP)[34] – the legislation concretely enables all stakeholders engaged in strategic operational dynamics to contribute to the establishment of an adequate level of cybersecurity within the country. This objective is essentially achieved by imposing a series of obligations on those entities included within the perimeter. These obligations pertain to the disclosure of technological equipment, the notification of cyber incidents, the technical adaptation of information infrastructures and, moreover, submission to supervision by

[33] B. Bruno, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, in Federalismi.it, no. 14/2020, 11 ff.

[34] See Article 1, c. 1, Decree-Law. 105/2019, whereby "*In order to ensure a high level of security of the networks, information systems and computer services of public administrations, public and private entities and operators having an establishment in the national territory, on which the exercise of an essential function of the State depends, or the provision of a service essential for the maintenance of civil, social or economic activities fundamental to the interests of the State, and from the malfunctioning, interruption, even partial, or improper use of which harm to national security may result, the national cybersecurity perimeter is hereby established*".

the competent authority with respect to the activities performed and the procurement of ICT goods and services

2.1. *The National Security Perimeter: adaptive and covert cybersecurity*

One may conceptualise the National Security Perimeter as a mobile boundary, within which the State exercises authoritative and supervisory powers over selected entities, while a degree of autonomy persists outside its confines. This system is, by design and necessity, characterised by confidentiality: the list of designated entities is not published but, rather, notification of inclusion is provided individually and the right of access to administrative documents does not apply in this context[35]. This is the Cybernetic National Security Perimeter (PSNC/CNSP), established to safeguard the strategic interests of the State. Inclusion and continued presence within the perimeter are determined – and cannot be negotiated – by the essential nature of the function performed or the service provided. However, this characteristic is inherently subject to a certain degree of "volatility": a newly introduced function or service, or an evolution in its practical application, may render essential what previously was not considered as such.

In light of this open-ended reference, it is Prime Ministerial Decree No. 131 of 30 July 2020[36] – which applies to "*public administrations, public and private entities, and operators […] having an office in the national territory*" – that establishes the criteria. An essential function is defined as one that "*assigns tasks aimed at ensuring the continuity of the action of the government and constitutional bodies, internal and external security and the defence of international relations, security and public order, the administration of justice, and the functionality of the economic, financial, and transport systems*". An essential service, in turn, is defined as the "*maintenance of civil, social, or economic activities that are funda-*

[35] See Article 1, c. 2-bis, Decree-Law 105/2019, whereby "*The list of identified subjects* […] *is contained in an administrative act, adopted by the President of the Council of Ministers, upon proposal of the CIC, within thirty days from the date of entry into force of the Decree of the President of the Council of Ministers referred to in paragraph 2. The aforementioned administrative act, to which the right of access is excluded, is not subject to publication, it being understood that each person is given, separately, notice without delay of their inclusion in the list* […]".

[36] Prime Ministerial Decree, No. 131 of 30 July 2020 on "*Regulations on the National Cybersecurity Perimeter*".

mental to the interests of the State"[37]. In both definitions, it is necessary to verify the existence of the precondition that the function or service deemed essential depends on networks, information systems or computer services, the interruption or impairment of which could be detrimental to national security. This requirement, in fact, corresponds to the ultimate interest protected by the relevant legal provision. The process of identifying and "enrolling" subjects within the National Cybersecurity Perimeter is thus carried out through the exercise of authoritative powers by the relevant sectoral administrations (the Presidency of the Council and individual Ministries, depending on the strategic activity involved)[38] and through a process of gradual or discretionary assessment that considers, for each function or essential service, the degree of prejudice to national security in the event of interruption or compromise. Such an organisational model is inherently flexible and lends itself to the continual updating of the Perimeter's contents, both in terms of essential functions and services and in terms of the subjects enrolled. This adaptability enables the model to respond to the rapid technological evolution characterising the various sectors involved and, above all, to emerging cyber threats.

A similar approach to adaptability is reflected in provisions requiring the constant updating – at least annually, as mandated by law – of the "list of networks, information systems, and IT services" associated with functions and services already deemed essential. This is intended to prevent situations in which the upgrading or renewal of technological infrastructure by an individual subject within the perimeter, if not promptly communicated, could serve as a "backdoor" for dangerous intrusions into an

[37] In particular, it is an essential service in the case of: activities instrumental to the exercise of essential functions of the State; activities necessary for the exercise and enjoyment of fundamental rights; activities necessary for the continuity of supplies and the efficiency of infrastructure and logistics; research activities and activities relating to productive realities in the field of high technology and in any other sector, whether they are of economic or social importance, also for the purposes of guaranteeing national strategic autonomy, competitiveness and the development of the national economic system (Article 2, Prime Ministerial Decree 131/2020).

[38] The sectors of activity relevant to the perimeter are indicated in Article 3, c. 1, Prime Ministerial Decree, No. 131/2020: governmental sector, concerning, within the activities of the State administration, the activities of the administrations that are part of the CISR – Interministerial Committee for the Security of the Republic; further sectors, referring to activities such as: a) interior; b) defence; c) space and aerospace; d) energy; e) telecommunications; f) economy and finance; g) transport; h) digital services; i) some critical technologies ex EU Regulation 2019/452; j) social security/labour institutions.

information system that was otherwise expected to be protected. It is evident, therefore, that no information infrastructure – least of all those of strategic importance within the perimeter – can be considered definitively secure: rather, it is a continuous race against time, marked by an ongoing contest between cyber threats, defensive measures and the updating of systems in terms of hardware, strategies, and software[39].

However, it must always be borne in mind that the substantial interconnection among actors within the cybersecurity perimeter – an implicit assumption and a direct consequence of the national cybersecurity regulatory framework – constitutes both an advantage, in terms of responding to systemic threats and a vulnerability ("*vulnus*"), in the event of highly diffuse attacks. This duality is particularly significant with respect to what now constitutes the country's nerve centre and strategic information hub.

[39] The regulatory framework that integrates and specifies the regulations introduced on the PSNC by Decree Law105/2019 is, in addition to the Prime Ministerial Decree 131/2020, composed of further provisions that, for example, impose on the perimeter participants the obligation to notify the Computer Security Incident Response Team ("CSIRT") established at the ACN in the event of incidents affecting ICT assets falling within the list prepared by the perimeter participants (see the Prime Ministerial Decree No. 81 of 14 April 2021 "*Regulations on the subject of notifications of incidents impacting on networks, information systems and information technology services referred to in Article 1, paragraph 2, letter b, of Decree-Law No. 105 of 21 September 2019*"), the obligation to notify the procurement or purchase of ICT systems and services (see D.P.C.M. 15 June 2021 on "*Identification of the categories of ICT goods, systems and services intended to be used in the National Cybersecurity Perimeter*", which "*identifies the categories in relation to which the entities included in the perimeter that intend to proceed, also through the central purchasing bodies to which they are required to have recourse, to the awarding of supplies of ICT goods, systems and services, intended to be used on networks, information systems and for the performance of IT services […], they shall notify the CVCN [National Evaluation and Certification Centre established at the Ministry of Economic Development] or the CV [Evaluation Centres established at the Ministry of Defence and the Interior]* […]"), or they shall implement and define the technical-operational procedures of evaluation by the aforesaid CVCN/CV (see D.P.C.M. No. 54 of 5 February 2021 – "*Regulations implementing Article 1, paragraph 6, of Decree-Law No. 105 of 21 September 2019, converted, with amendments, by Law No. 13*") and those of accreditation of the Accredited Testing Laboratories – LAPs and CVs, entities that, together with the CVCN, are responsible for the evaluation and execution of any hardware/software tests deemed necessary for the purpose of the use of a given asset within the perimeter (see Presidential Decree 18 May 2022, no. 92 on "*Regulations on the accreditation of testing laboratories and the links between the National Assessment and Certification Centre, the accredited testing laboratories and the Assessment Centres of the Ministry of the Interior and the Ministry of Defence*").

2.2. *PNRR, the new agency and the limit of governmental power*

The National Recovery and Resilience Plan (PNRR) includes, among its interventions, the establishment of an Italian cybersecurity system as part of a broader process of public administration renewal[40].

The allocation of resources intended to strengthen the country's cyber protection amounts to approximately EUR 620 million, of which EUR 241 million is dedicated to the creation of a national cybersecurity infrastructure, EUR 231 million to the enhancement of the operational structures of the National Cybersecurity Perimeter and EUR 150 million to the improvement of national cyber defence capabilities within the Ministries of the Interior, Defence, the Guardia di Finanza, Justice, and the Council of State.

A fundamental step in this modernisation process is the establishment of the National Cybersecurity Agency (ACN/NCA), created by Decree Law No. 82/2021 with the mandate to "protect national interests in the field of cybersecurity." The Agency is a public law entity endowed with broad regulatory, administrative, patrimonial, organisational, accounting and financial autonomy. Its functions encompass coordination among various public entities involved in the sector, international cooperation, qualification and certification in the field of cloud services, supervision and imposition of sanctions in the implementation of the National Cybersecurity Perimeter, preparation of the National Cybersecurity Strategy and the role of competent authority for the security of networks, information systems and electronic communications. Additionally, the Agency undertakes extensive consultative activities on legislative and regulatory initiatives in the field and is empowered to adopt guidelines, operating in close collaboration with the Prime Minister, for whom it acts, *de facto*, as the implementer of the cybersecurity competences assigned to the office[41].

[40] Cybersecurity is one of the 7 investments of the Digitisation of Public Administration, the first axis of intervention of Component 1 "*Digitisation, Innovation and Security in PA*" included in Mission 1 "*Digitisation, Innovation, Competitiveness, Culture and Tourism*".

[41] Article 2, Decree Law 82/2021 clarifies in c. 1 that "*The President of the Council of Ministers is exclusively attributed: a) the top management and general responsibility for cybersecurity policies* […]*",* while the following Article 5, c. 2, defines the operational relationship that creates the functional connection between the Prime Minister's Office and ACN, in the part where it states that "*The President of the Council of Ministers […] avails himself of the Agency for the exercise of the competences referred to in this decree* […]".

This last characteristic is particularly instructive in understanding the role of the ACN/NCA. Despite its designation, the National Cybersecurity Agency does not fully conform to the general model established by Legislative Decree No. 300/1999, which pertains to instrumental bodies lacking legal personality and subject to ministerial supervision. In contrast, the ACN/NCA, in addition to its public legal status, is directly subject to the direction of the Prime Minister[42], thereby aligning its structure more closely with that of the national intelligence apparatus – specifically, the National Security Information System which is headed by the same Prime Minister[43].

The governmental centralisation of the cybersecurity function, therefore, not only clarifies the absolute inapplicability to the ACN/NCA of forms of independence comparable to those of regulatory authorities, but also exposes the management of this strategic sector to the vicissitudes associated with partisan interests that characterise political activity.

Of particular note is the delegation of certain cybersecurity functions[44] by

[42] In this regard, see what is provided for by Article 8 of Decree Law no. 82/2021, which, in paragraph 1, expressly establishes the Cybersecurity Nucleus within the ACN as a structure "*supporting the Prime Minister in matters of cybersecurity* […]", also noting the existence of a presidential power of appointment (Article 2, paragraph 1, letter c), Decree Law No. 82/2021, according to which "*The Prime Minister is exclusively responsible for: […] appointing and dismissing the Director General and Deputy Director General of the National Cybersecurity Agency* […]". 82/2021, according to which "*the President of the Council of Ministers is exclusively responsible for:* […] *appointing and dismissing the Director General and the Deputy Director General of the National Cybersecurity Agency* […] *after deliberation by the Council of Ministers*") and for directing and organising (Art. 2, c. 2, d.l. 82/2021 whereby "*2. For the purposes of exercising the competences […] and implementing the national cybersecurity strategy, the President of the Council of Ministers* […] *shall issue the directives for cybersecurity and issue any necessary provisions for the organisation and functioning of the National Cybersecurity Agency*").

[43] Regulated by Law no. 124/2007, the Information System for the Security of the Republic includes, under art. 2, c. 1, l. 124/2007, "[…] *President of the Council of Ministers,* […] *Interministerial Committee for the Security of the Republic (CISR)*, […] *Delegated Authority* […] *Department of Security Intelligence (DIS)*, […] *External Intelligence and Security Agency (AISE) and* […] *Internal Intelligence and Security Agency (AISI)*".

[44] These are functions that are not exclusively assigned by the regulatory norm. See Article 3, c. 1, Decree Law 82/2021, according to which "*The President of the Council of Ministers, if he deems it appropriate, may delegate to the Authority referred to in Article 3 of Law no. 124 of 3 August 2007, where established, hereinafter referred to as: 'Delegated Authority', the functions referred to in this Decree that are not exclusively attributed to it*".

the Prime Minister to the Delegated Authority for the Security of the Republic [45], who is responsible for intelligence matters [46].

Given the evident proximity between the domains of networks and information systems and the intelligence sector (with its inherent tendency towards secrecy), as well as the described similarities in governance (as exemplified by the delegation of functions), potential vulnerabilities may arise within the structure, particularly in the form of possible compromises regarding transparency (i.e. secrecy)[47]. This is especially relevant with respect to the rationale and circumstances surrounding the involvement of those entities "*ex officio*" enrolled in the National Cybersecurity Perimeter, who, as a result of such enrolment, are subject to a significant share of obligations.

3. *Public intervention in the cybersecurity sector*

The foregoing considerations underscore the absolute centrality of cybersecurity within the Europe-driven modernisation processes currently shaping the country, as well as within the dynamics of its regular functioning, which is robustly protected at the regulatory level. Moreover, the trend towards the progressive computerisation of society is now both undeniable and irreversible – a phenomenon markedly accelerated by the

[45] The delegation of functions took place with the Prime Ministerial Decree of 12 November 2022 ("*Delegation for the Security of the Republic, pursuant to Article 3 of Law No. 124 of 3 August 2007, to the Undersecretary of State to the Presidency of the Council of Ministers, Dr. Alfredo Mantovano*") but, unlike what happened previously, where the delegated authority was the expression of a technical competence (see the D.P.C.M./Prime Ministerial Decree 13 September 2021, with the assignment of the delegation to Prefect Gabrielli), on this occasion it is a political exponent of the government.

[46] In particular, those functions (Art. 1, c. 3 and 3-bis, Law 124/2007) conferred on the Delegated Authority for the Security of the Republic, on the basis of which the President of the Council of Ministers "*3.* […] *provides for the coordination of the policies of the information for security, issues directives and, after consulting the Inter-ministerial Committee for the Security of the Republic, issues any necessary disposition for the organization and functioning of the Information System for the Security of the Republic. 3-bis.* […] *shall issue directives to the Department of Security Intelligence and the Security Intelligence Services to strengthen intelligence activities for the protection of tangible and intangible critical infrastructures, with particular regard to national cyber protection and cybersecurity*".

[47] It should be noted that Decree Law105/2019 already provides for the exclusion of the right of access with reference to the administrative act that identifies the subjects forming part of the PSNC (Art. 1, c. 2 bis).

distancing requirements imposed during the COVID-19 pandemic and by the advent of new communication and intelligent, albeit artificial, data processing technologies. It logically follows that the role of cybersecurity strategies in ensuring the orderly conduct of social and institutional activities is of growing importance. As all activities increasingly migrate to the Internet, the Internet itself tends to become a protected asset of public interest. Consequently, the State requires a suite of operational instruments to guarantee the performance of functions and services deemed essential within its strategic sectors. In pursuing this objective, the State necessarily interacts not only with its own structures but, increasingly, with private entities that contribute to the functioning of the national system by operating daily in both sensitive and non-sensitive sectors.

The concrete exercise of these instruments – particularly in relation to companies and individuals – constitutes a clear example of public sector intervention in the national economy. Several instruments have been identified through an examination of the relevant legal provisions, which the State may employ to pursue the public interest in the field of cybersecurity. An analysis of the salient features of these instruments will be provided below.

3.1 *The "golden power"*

The so called "golden power" is a powerful governmental instrument introduced into the Italian legal system by Legislative Decree No. 21/2012 (as amended by Law No. 56 of 11 May 2012), and has since undergone numerous modifications, resulting in a progressive extension of its scope of application. Through the exercise of golden power, the State may intervene in the activities of companies operating in strategic sectors, to the extent of prohibiting certain actions (by expressly exercising a power of veto, whereas the general regulatory framework would otherwise provide for a mechanism of tacit assent to notified strategic economic operations) or, alternatively, subjecting such actions to specific conditions (by exercising a prescriptive power) with respect to a range of corporate acts and operations that would typically fall within the domain of private autonomy.

Accordingly, golden power constitutes a highly pervasive instrument in terms of its scope[48] and is equally invasive in its effects.

[48] The scope of application of golden power has been the subject of renewed interest on the part of administrative jurisprudence, with particular reference to the relationship

At present, the governmental "golden power" may be exercised[49] over a wide range of corporate acts and operations – including the acquisition of shareholdings, mergers, demergers, transfers, incorporations, changes of registered office, amendments to corporate purpose and by-laws, assignment of rights, imposition of restrictions, and dissolution – where such acts are undertaken by legal entities, including private companies, within sectors deemed strategic[50]. These sectors include networks,

between this institution, the regulatory norm and the principle of legality, stably interpreted in terms of the necessary peremptory nature of the application hypotheses of the special power (in the sense of requiring a prior regulatory categorisation of a certain sector as "strategic", see T.A.R. Piemonte, section I, 13 July 2021, no. 727). Specifically, an italian court, departing from the previous orientation, clarified how "*the drafting technique used to identify the assets* […] *represents an adequate compromise between the protection of freedom of enterprise and the guarantee of national security and takes into account the impossibility of a precise and detailed cataloguing of strategic assets*" (see T.A.R. Lazio-Rome, section I, 13 April 2022, no. 4486), an interpretation that has found further support in Council of State, section IV, which, in its ruling of 9 January 2023, no. 289, affirmed that with regard to the institution of golden power "*we are outside the field of criminal law (which imposes, as is known, the need for a particular taxability in the enucleation of the case law), falling outside the legislation […] any afflictive purpose; likewise, there is no imposition of a financial benefit under Article 23 of the Constitution, but the mere legislative provision of a safeguard to verify the compatibility of private economic initiative with social utility (art. 41 of the Constitution), a broad expression which certainly includes the national interest with regard to 'goods and strategic relations' as identified by law*". On this point, see A. Paccione, *Il Golden Power e il principio di legalità*, *Giornale di diritto amministrativo*, no. 5/2022, 659 ff., who records "[…] *the need to partially sacrifice the rigorous predetermination of the application prerequisites of golden power in order to guarantee an efficient protection of the public interest in security* […]*, although the risk 'of an escape of the exercise of authoritative powers from the framework of constitutional and Euro-unitarian principles that regulate administrative activity' remains*" (translated by the author).

[49] Also *ex officio*, in the absence of the prescribed notification of the potentially strategic transaction (pursuant to Article 1, paragraph 8-bis, of Decree Law No. 21/2012) and having a special inspection power (pursuant to Article 2-bis: "*In order to gather elements useful for the application of Articles 1, 1-bis and 2, the Coordination Group* […] *may request public administrations, public or private entities, companies or other third parties in possession of such information, to provide information and to produce documents*").

[50] Several measures have, over time, implemented and better specified the golden power discipline, including in particular d.l. 148/2017 later converted into Law 172/2017 (which extended its applicability to "technology-intensive sectors" such as critical or sensitive infrastructure, including data storage and management, financial infrastructure; critical technologies, including artificial intelligence, robotics, semiconductors, technologies with potential dual-use applications, network security, space or nuclear technology; security of supply of critical inputs; access to or ability to control sensitive information),

strategic infrastructures and critical technologies, among which cybersecurity is expressly included[51]. Such acts are subject to intervention where they are capable of posing a serious threat to the essential interests of the State or endangering security or public order.

d.l 105/2019 later converted into Law 133/2019 (which summarised the taxonomy introduced in 2017 and merged it into the broad category of "*security and* […] *operation of networks and facilities* […] *in the areas referred to in Article 4(1) of Regulation EU 2019/452 of the European Parliament and of the Council of 19 March 2019*", which in lett. b) refers to and expressly includes the "cybersecurity" sector), Decree Law 23/2020 (i.e. the so-called Liquidity Decree, which in Art. 15 introduced an extension of the scope of application of the discipline, defined as "strengthened Golden Power"), the related D.P.C.M. 179/2020 and 180/2020 (which specified some procedural and applicative steps, in particular art. 3 of the D.P.C.M. 180/2020 provided that "*the assets of strategic importance in the communications sector are identified in the dedicated networks and in the public access network to end users in connection with metropolitan networks, service routers and long distance networks, as well as in the facilities used for the provision of access to end users of the services falling under the universal service obligations and broadband and ultra-wideband services, and in the related contractual relationships*"), Decree Law no. 21/2022 (i.e. the so called Energy Decree, converted with amendments by Law no. 51 of 20 May 2022 and adopted to counter the effects of the Russian-Ukrainian crisis, which stabilised the scope of application of the instrument and – like the subsequent Prime Ministerial Decree no. 133/2022 – introduced a number of procedural simplifications), Decree Law No. 187/2022 (converted with amendments by Law No. 10 of 1 February 2023, which provided for the possibility of access to forms of state economic aid in favour of companies subject to the exercise of golden power).

[51] In June 2023, the Italian government exercised its prerogatives in terms of golden power, in the form of the imposition of prescriptions, in an important corporate transaction involving China National Tire and Rubber Corporation, Ltd. in reference to the shareholders' agreement on the governance of the company Pirelli & C. S.p.A. Specifically, it concerned prescriptions relating to the protection of the strategic asset consisting of cyber sensors that can be implanted in tyres. According to the press release dated 16/6/2023 (at governo.it), in fact, "*These sensors are capable of collecting vehicle data regarding, among other things, road layout, geolocation and the state of infrastructure. The information thus collected can be transmitted to cloud processing systems and supercomputers for the creation, through artificial intelligence, of complex digital models that can be used in cutting-edge systems such as smart cities and digital twins. The relevance of this cyber technology can be identified in a variety of sectors: industrial automation, machine-to-machine communication, machine learning, advanced manufacturing, artificial intelligence, critical sensor and actuator technologies, Big Data and Analytics. For these sectors, cyber emerges as a critical technology of national strategic importance. The misuse of this technology can entail considerable risks not only for the confidentiality of user data, but also for the possible transfer of security-relevant information. The Government's prescriptions are intended to create a network of measures that protect: the autonomy of Pirelli & C. S.p.A and its management; the security of procedures; the protection of information of strategic importance; and the know-how possessed by the company*" (translated by the author).

Specifically, the technology of broadband electronic communications, such as 5G, as well as cloud computing and other strategic assets in the field of cybersecurity (which may be identified in the future), are subject to a further dedicated application of the "golden power"[52]. In these cases, the focus shifts to the contractual phase concerning the acquisition of goods, services, and components necessary for the design, implementation, maintenance, and management of the relevant infrastructure. This mechanism, once again in the name of the national interest[53], operates to limit the autonomy typically enjoyed by companies during the procurement phase.

3.2. *The Presidential shutdown*

The exclusive prerogative of the President of the Council of Ministers, although normatively circumscribed both in duration ("*for the time strictly necessary for the elimination of the specific risk factor or its mitigation*") and in scope ("*according to a criterion of proportionality*"), consists in the authority – conferred by Article 5 of Decree Law No. 105/2019 – to order the so called "shutdown" of equipment and products included within the National Security Perimeter, insofar as such assets are employed in networks, systems or for the provision of services subject to cyber threat. This power, which may entail either total or partial deactivation of the national cyber infrastructure, is of an exceptionally incisive character, to the extent that it may be exercised in derogation of any other provision in force.

It is, moreover, an extraordinary measure[54], the immediate effect of which is to the detriment of the economy and of those business or institu-

[52] See Article 1 bis, Decree Law 21/2012.

[53] For B. Carotti, *Sicurezza cibernetica e Stato-nazione*, cited above, 639, "*the question of the nationality of proprietary control and the origin of technologies testifies to the revival of a very rigid State-centric and national conception*", "*a consequence of the renewed conceptual persistence of the 'nation-State'*" (translated by the author).

[54] See Article 5, c. 1, Decree Law. 105/2019, whereby "*The President of the Council of Ministers, in the presence of a serious and imminent risk to national security related to the vulnerability of networks, information systems and computer services, upon the deliberation of the Interministerial Committee for the Security of the Republic, may nevertheless order, where indispensable and for the time strictly necessary for the elimination of the specific risk factor or its mitigation, by way of derogation from any provision in force, in compliance with the general principles of the legal system and in accordance with a criterion of proportionality, the total or partial decommissioning of one or more apparatuses or products used in the networks, systems or for the performance of the services concerned*".

tional entities connected to the affected service or system. Precisely in view of its far-reaching consequences, the exercise of this prerogative is subject to a prior deliberation by the Interministerial Committee for the Security of the Republic (CISR)[55], which is charged with assessing the existence of a serious and imminent risk to national security, specifically as regards the vulnerability of networks, information systems and IT services.

3.3. *Information and reporting obligations*

The entities involved in the management of national cybersecurity, particularly those registered "*ex officio*" within the National Security Perimeter, are subject to a comprehensive system of sanctions – primarily pecuniary, but also prohibitory and criminal in nature – as well as regulatory oversight[56], designed to ensure compliance with several key obligations.

First, there exists an obligation to conduct a census and subsequently report on the technological assets available to these operators. Members of the National Security Perimeter are required to prepare and update, at least annually, a "list of networks, information systems, and IT services" which must also include the relevant architecture and components. The purpose of this requirement is to facilitate continuous monitoring of the infrastructure, thereby enhancing both preventive and responsive capacities in relation to cyber threats.

[55] The presidential prerogatives, in compliance with Article 5 of d.l. 105/2019, therefore provide for an *ex ante* check by the CISR – Interministerial Committee for the Security of the Republic in terms of the seriousness of the threat, which is followed by an *ex post* check by the COPASIR – Parliamentary Committee for the Security of the Republic, which is specifically informed (on this point, see Art. 5, c. 1-bis, d.l. 105/2019, whereby "*The President of the Council of Ministers shall inform within thirty days the Parliamentary Committee for the Security of the Republic of the measures ordered* […]". For a reconstruction of the functions initially assigned to CISR and COPASIR and the relations between these two bodies, also with respect to the figure of the Prime Minister, see: T.F. Giupponi, *Servizi di informazione e segreto di Stato nella legge n. 124/2007*, in AA.VV., *Studi in onore di Luigi Arcidiacono,* Vol. IV, Torino, Giappichelli, 2010, 1677 ff. (also at *forumcostituzionale.it*); M. Malvicini, *Sicurezza della Repubblica e forma di governo parlamentare. Il Rapporto tra presidente del Consiglio dei ministri e Copasir alla luce dei più recenti interventi legislativi (legge 11 dicembre 2015, n. 198)*, in *Forum Quaderni Costituzionali – Rassegna, 5/2016* (at *forumcostituzionale.it*).

[56] A. Renzi, *Sicurezza nazionale cibernetica: uno sguardo al documento annuale*, in Observatory on the Digital State of 09/06/2020, at *irpa.eu*, who speaks of "*investment screening and technology screening*"(translated by the author).

Second, there is an information obligation towards the National Assessment and Certification Centre (CVCN), established at the Ministry of Economic Development, with respect to technological procurements deemed necessary by the operators. Through this mechanism, a prior assessment of cyber vulnerability is conducted, which may result in the suspension or significant conditioning of the procurement process.

Finally, there exists a duty to promptly notify computer incidents that have affected networks, information systems or IT services. This obligation is intended to counteract malicious events and prevent their proliferation and is fulfilled through notification to the Computer Security Incident Response Team (CSIRT), established at the National Cybersecurity Agency (ACN/NCA)[57].

4. *Conclusions*

The census of public data infrastructure assets conducted in 2020 revealed that 95% of public administration data centres fail to meet the minimum security and reliability standards required for the provision of services and the management of information[58]. It is therefore evident that the domain of cybersecurity, together with the protection of national computer networks, is destined to assume an increasingly strategic role within the organisational and economic dynamics that shape contemporary society and public administration[59].

[57] The regulation of the obligations incumbent on the persons registered in the PNSC can be found in Article 1, Decree Law 105/2019, in particular in c. 2, letter b) (preparation of lists), c. 3, letters a) and c. 3-bis (notification of events) and, finally, in c. 6, letter a) (notification to the CVCN).

[58] See: Hearing of the Minister for Technological Innovation and Digital Transition Vittorio Colao, dated 13/04/2021, at the Transport Commission of the Chamber of Deputies. The data, taken from the document drawn up by AGID in 2020 entitled "Census of PA ICT assets", show that 13 % of data centres were built before 1996, 28 % between '96 and 2005, 46 % between 2006 and 2015, and 13 % after 2015, with 64 % of the data centres surveyed having undergone final modernisation after 2015 (but with alarming 36 % still before 2015).

[59] The condition of substantial inadequacy of the public ICT assets, revealed by the AGID Census of 2020, appears to be gradually improving thanks to the projects prepared and the liquidity provided under the PNRR, as confirmed by the findings contained in the AGID 2023 Report (published in August 2023, at *agid.gov.it*) on ICT Expenditure in the Italian Public Administration. The report, in fact, which considers a cluster of 77 central, regional and local administrations capable of intercepting over 90% of PA ICT spending,

This is an issue that the European Union has long since identified as a priority; nevertheless, owing to the specificity of the interests at stake and the sensitivity of the data potentially involved, it remains of undeniable and acute relevance at the domestic level. Consider, for instance, the vast array of information that traverses the Internet today, irrespective of whether it pertains to connections or services within the public or private sphere: personal data of every kind, including highly sensitive information such as healthcare records, access credentials for payment services, credit card numbers, IBANs, purchasing habits derived from e-commerce platforms, Internet browsing histories, geolocation data and user profiling. This enumeration is by no means exhaustive.

shows a growing trend in PA ICT spending in the period 2022-2024 (+5.2%). Specifically, 2021 will see the most significant increase (+10.1%), after the lower growth that occurred in 2020 and which was linked to the COVID-19 pandemic that had slowed investments. In addition, "*a significant proportion of institutions focused on renewing networks and infrastructure, to support smart working, which was still the predominant mode of work in 2021, given the prolonged pandemic. These were followed, in terms of project numbers, by the evolution of databases and reporting and by data centre renewal and cloud transition projects*" (AGID Report 2023, cited above, 9). It should be noted, then, that "*The project choices made by the PA, in the three-year period 2021-2023, have seen 'Platforms' as the prevailing sphere, both from a numerical point of view (279 interventions) and from a resource point of view (2.2 billion euros), with the aim of supporting the rationalisation of PA back-office or front-end processes and creating simpler and more homogeneous digital services*" (AGID Report 2023, cited above, 93). Finally, from the point of view of cybersecurity, the AGID report highlights how "*Total expenditure on systems and services for security and continuity of operation exceeded, within the panel, 193 million euros in 2022, an increase of over 10% compared to 2020. The resources allocated to this area see a consolidation of growth in the two-year period 2023-2024 […]. Overall, it is the central government (73% of the total) and the regions and autonomous provinces (around 22%) that contribute most to the total expenditure in 2021, while local authorities contribute marginally with the remaining 5%. Overall, there is a 6% incidence of spending on security compared to overall ICT spending, thus showing an improvement over previous surveys, testifying to the growing attention of public administrations to cybersecurity issues. Most of the expenditure is attributable to Disaster Recovery and Business Continuity systems (on average, in the four years covered by the survey, they accounted for about 38% of the total), the importance of which was further accelerated by the healthcare emergency, with a growing trend in the last two years of the survey. Allocating the largest resources in this particular area are the CAPs with about EUR 240 million over the four years 2021-2024. The second largest category of expenditure, with a total of 257 million euros declared in the four years covered by the survey, is Operational Infrastructure Security, with the aim, on the part of the Administrations, of increasing the security of infrastructures. In particular, it is the LAPs that allocate to this area, on average over the four years, 53% of their security resources, equal to almost 6 million euros*" (AGID Report 2023, cited above, 82 ff.).

Indeed, the National Recovery and Resilience Plan (PNRR) itself enumerates, among its objectives and conditionalities, the widespread digitisation of public administration – with an allocation of approximately EUR 10 billion – and the digital transformation of businesses, for which the allocated resources amount to EUR 24 billion. These processes, by virtue of the inseparable nexus between digital technologies and the Internet, are inextricably linked to the imperative of cybersecurity.

Nevertheless, the Internet daily demonstrates itself to be a tool of considerable potency in generating economic value – for instance, in 2020, the Internet of Things (IoT) alone produced an economic value of EUR 6 billion in Italy, rising to EUR 8.3 billion in 2022[60], while in the first half of 2024, the global digital market recorded a value of EUR 39.2 billion[61]. Yet, this very instrument remains fragile in its resilience to external threats. Cyberattacks perpetrated via the Internet – whether for extortion, the trafficking of illicitly obtained data, or subversive, disruptive or even terrorist purposes – are, as previously observed, in constant ascent. Such phenomena represent a significant criticality for the orderly functioning of the national economy and the State apparatus as a whole, thereby necessitating, and increasingly so, a proactive countervailing role on the part of the State. The State must, in turn, be capable of coordinating and engaging with the private sector, particularly with companies, given

[60] Source: Internet of Things Observatory of the School of Management of Politecnico di Milano – IoT Research 2023-2024, according to which "*the largest slice of the market is represented by Smart Cars, with a turnover of 1.4 billion euros, or 17% of the total. In the second place, IoT applications in the utility world (Smart Metering and Smart Asset Management) with 1.37 billion euros, growing but now close to saturation: 1.1 million additional connected gas meters in households (84% of the total fleet) and 1.7 million second-generation smart electric meters (64% of the total) will be installed in 2022. This is followed by Smart Building (1.3 billion), Smart City (830 million), Smart Factory (780 million), Smart Home (770 million), Smart Logistics (715 million) and Smart Agriculture (540 million). The areas that are growing the most within the IoT market, however, are Smart Agriculture (+32%), Smart Factory (+22%) and Smart Building (+19%). There are 124 million actively connected objects in Italy, just over 2.1 per inhabitant. At the end of 2022, there will be 39 million cellular IoT connections (+5% compared to 2021) and 85 million connections enabled by other communication technologies (+15%). Among these, a significant boost comes from LPWA (Low Power Wide Area) networks, which see a 20% growth in one year, from 2 to 2.4 million connections. Also, this year, the biggest push on the market comes from applications using non-cellular communication technologies, 4.5 billion, +15%. More moderate growth, +11%, for applications that exploit cellular connectivity, whose market value reaches EUR 3.8 billion*".

[61] According to Anitec-Assinform report, Digital in Italy, 2024, at *anitec-assinform.it*.

that the discipline of cybersecurity constitutes a multilevel and infra-territorial system, inherently complex and organic. This system is safeguarded from below by the infrastructures and expertise of market operators, yet it requires ever greater support and guarantees from governmental prerogatives. Ultimately, the end user – be it the citizen or the small business – represents the final link in this chain. It is the end users – citizens and small businesses – who most immediately perceive inefficiencies, for example, when the Lazio Region's website fails to permit the booking of COVID-19 vaccinations, or when a phishing attack succeeds in encrypting their data and subsequently demands a ransom for decryption.

In reality, however, it is the broader community – comprising citizens, public administrations, workers, and companies – that ultimately bears the greatest aggregate costs. Consider, for instance, the case of Luxottica, one of Italy's largest enterprises, which was compelled to halt production in September 2020 due to data theft, with all the attendant economic and logistical repercussions. Similar malicious events have affected ACEA Energia in March 2023 and the Gestore Servizi Energetici (GSE) in July 2023.

Within this context, the substantial – and, by now, nearly total – interconnection between the various public and private networks across the national territory gives rise to an additional problematic dimension: the "contagiousness" of computer infections, that is, their capacity for diffusion through mechanisms that are, in practice, quite simple, such as an apparently innocuous email or the redirection of a user to a website that appears authentic but is, in fact, deceptive. The National Cybersecurity Perimeter is thus conceived as the State's response to this category of threat, and the establishment of the National Cybersecurity Agency further attests to the institutional dynamism and heightened attention devoted to the sector.

Within the perimeter, the State "involves" certain companies operating in strategic sectors – indeed, it mandates their participation, a fact which underscores the significance of the protected interests at stake – and integrates them into a joint cyber defence programme. This programme imposes obligations to report cyber incidents, to conduct a census and update technological equipment, and even to review the adequacy or effectiveness of supplies of goods and services deemed "cyber-relevant."

Accordingly, the preferred solution for combating cybercrime and safeguarding the security of electronic networks must be identified, from the very design phase of network infrastructure ("security by design"), in

the close coordination between public authority and private autonomy. The latter is, without doubt, constrained in certain prerogatives previously taken for granted, such as the now-diminished freedom to conclude sales agreements concerning strategic assets.

In some instances, however, coordination alone proves insufficient, necessitating a more assertive role for the State. On the one hand, the regulatory framework of the National Cybersecurity Perimeter overlaps with that governing critical technologies, wherein the government, upon being duly informed, is likewise empowered to intervene with security checks on goods, services and technological components that a company intends to procure. On the other hand, the imperative to protect national interests, security, and public order in so called strategic assets – such as computer networks – justifies even more invasive public intervention in the economy. Through the exercise of "golden power," the State may, in fact, prohibit or impose conditions upon passive corporate acts and transactions undertaken by companies with foreign entities, or those effectively disguised as such[62].

In this manner, however, there arises the risk of a thinly veiled resur-

[62] It should be noted that the COVID-19 emergency legislation included, in the notion of foreign investment relevant to the exercise of golden power, also those transactions in which the buyer is directly or indirectly controlled by a public administration of an EU member State (see Art. 15, c. 3 bis, lett. c, d.l. 23/2020), while in the context of the fight against the effects of the Russian-Ukrainian crisis to be extended, with d.l. 21/2022 converted with l. 51/2022, was the notion of "subject outside of the European Union" (see d.l. 21/2012, art. 2, c. 5-bis, whereby "*For the purposes of Article 1 [Special powers in the fields of defence and national security] and of this Article [Special powers inherent in strategic assets in the energy, transport and communications sectors], subject outside of the European Union means:* […]*; (b) any natural person who is a national of a member State of the European Union and who does not have his or her residence, usual place of abode or principal place of business in a member State of the European Union or the European Economic Area or who is not otherwise established there;* […]; […]; *d) any legal person that has its registered office or place of business or its principal place of business in a member State of the European Union or the European Economic Area, or is otherwise established there, and is controlled, directly or indirectly, by a natural person or a legal person referred to in subparagraphs (a), (b) and (c); (e) any natural person or legal person who is a national of a member State of the European Union or of the European Economic Area and who has established his or her residence, habitual abode, registered office or place of management or principal place of business in a member State of the European Union, or who is in any event established therein, where there is evidence of evasive conduct with respect to the application of the rules set forth in this Decree*". For an in-depth and insightful analysis of the foreign direct investment phenomenon, see G. Napolitano, *The regulation on the control of foreign direct investment: in search of European sovereignty in the global economic arena*,

gence of protectionism[63], a concern already articulated by the most authoritative doctrine, which cautions against the allure of dirigisme and technological nationalism – tendencies that conflate "government" with "state" and expand the perimeter of the latter solely to augment the power of the former[64].

The exercise of extraordinary – indeed special – powers, by definition and under constitutional principles, necessitates the existence of an actual and concrete threat to national security. Such a requirement is not readily discernible within the ordinary market dynamics encountered by any enterprise of significant scale operating internationally. This is especially true in a context characterized by pervasive interconnection, not only in information technology but also in commerce and industry.

Conversely, the presidential prerogative of cybernetic "shutdown" is far more consistent with its intended purpose: it is a governmental power that, while undoubtedly intrusive and detrimental to private initiatives, is circumscribed in both duration and scope and is characterized by its remedial or mitigative function in response to a malicious cyber event of manifest and objective gravity.

Accordingly, when the State elects – or deems it necessary – to regulate or otherwise affect the exercise of private activity, its intervention may assume various forms. In certain instances, it is a gentle, almost pa-

in *Rivista della Regolazione dei Mercati*, issue no. 1/2019, 2 ff. On the topic of golden power see also: G. Scarchillo, *Golden Powers e settori strategici nella prospettiva europea: il caso Huawei. Un primo commento al Regolamento UE 2019/452 sul controllo degli investimenti esteri diretti*, in *Diritto del Commercio Internazionale*, no. 2/2020, 569 ff.; R. Chieppa, *La nuova disciplina del golden power dopo le modifiche del decreto-legge n. 21 del 2022 e della legge di conversione 20 maggio 2022, n. 51*, in *Federalismi.it*, no. 16/2022; Presidency of the Council of Ministers, Report to Parliament 2022 on special powers, *governo.it*, 5 ff.; L. Torchia, *Politica industriale e regolazione*, in *Rivista della Regolazione e dei Mercati*, no. 1/2015, 1 ff. (and, in particular, 4, where the instrument is defined as an "exorbitant" power).

[63] A phenomenon that Italy had already experienced in the fascist period, with Law 141 of 12 January 1933. On the protectionist tendencies of individual states, see L. Arnaudo, *A l'économie comme a la guerre. Note su golden power, concorrenza e geo-economica*, in *Mercato Concorrenza Regole*, no. 3/2017, 435 ff. Still on the topic of golden power, see: M. D'Alberti, *Il golden power in Italia: norme ed equilibri*, in G. Napolitano (ed.), *Foreign Direct Investments Screening. Il controllo sugli investimenti esteri diretti*, Bologna, Il Mulino, 2019, 86 ff.; G. Napolitano, *I golden powers italiani alla prova del Regolamento europeo*, ivi, 121 ff.

[64] Interview with Sabino Cassese: "Tim-Vivendi e il golden power? Attenzione ai nuovi nazionalismi", Corriere della Sera dated 29/08/2017, p. 33.

ternalistic measure, designed to safeguard strategic structures and entities through the establishment of a "cybernetic enclosure", thereby enabling the State to maintain efficiency via continuous oversight, with the boundary between public and private interests becoming increasingly indistinct. In other circumstances, the intervention is more abrupt, yet justified, particularly when the "enclosure" risks collapse under the weight of digital attacks threatening systemic stability and the most prudent course of action is to "shut down" the country – or a portion thereof – to contain the damage. Finally, there are interventions that, while less perceptible, are considerably more disruptive, potentially undermining the delicate equilibrium underpinning the European freedom pact[65], especially when the core of economic initiative – namely, private property and its attendant prerogatives – is affected through methods and characteristics that have become structural rather than exceptional, as the regulatory framework has broadened[66].

Thus, while it may be asserted that the current cybersecurity system, as it is progressively implemented in Italy, constitutes a valid instrument for the protection of the national economy against cyber threats, it must also be acknowledged that certain fundamental concerns persist regarding its application. In particular, the response to the "fear of the foreign" ought not to consist in erecting new barriers to investment and trade, which risk unduly constraining or diminishing their commercial and industrial potential. Rather, the solution should be sought in the internal development of oversight mechanisms, of IT infrastructures and of the technical expertise necessary to ensure their efficacy, as well as in adherence to European freedoms and principles, to which Italy has long since pledged its commitment.

[65] In the article "Neostatalismo hi-tech. La fabbrica dei veti 5G", in L'Economia del Corriere della Sera, dated 05/08/2019, 7, Sabino Cassese notes how the most recent interventions in the field of golden power (especially those of the d.l. Brexit) could also be censured under a profile of unconstitutionality, given that the introduction of "blank" controls – without adequate definition of the criteria, purpose, limits and procedures of interference in private economic initiative – translates into a "*merely nominalistic respect of the Constitution*" and, therefore, into a circumvention of the reservation of law in a substantive sense prescribed, in this regard, by Article 41 Const.

[66] Think of the procurement phase of a company, which is inherent to the very essence of any entrepreneurial activity and therefore qualifies as decidedly ordinary and which, instead, is affected by the exercise of golden power as an extraordinary remedy.

in copertina: *Il banditore del Comune* pubblicizza l'apertura della scuola di diritto.
Affresco di Giulio Rolland (1890), Aula Magna Palazzo dell'Università (sede storica), Macerata.

euro 17,00

ISBN 979-12-235-0558-8