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