ItaliaOggi Sette

diffusione:88589
tiratura:133263



*In attesa di un regolamentazione Ue sull'intelligenza artificiale, il Parlamento decide lo stop*

# Sicurezza, privacy a rischio con il riconoscimento facciale

*PAGINE A CURA*
DI ANTONIO RANALLI

La crescente disponibilità di tecnologie di intelligenza artificiale per il riconoscimento facciale ha portato alcune amministrazioni comunali a pianificarne l'adozione per motivi di sicurezza, in zone particolarmente critiche delle rispettive città. Nel settore della pubblica sicurezza, le tecnologie di riconoscimento facciale funzionano abbinando le immagini facciali di un individuo ad un predefinito database di volti (c.d. watch list) allo scopo di identificare in modo univoco una persona. L'intero processo prevede tre passaggi fondamentali: rilevamento del volto, acquisizione del volto e corrispondenza del volto.Ma quest'esigenza di sicurezza può prevalere sulla riservatezza delle persone? Lo abbiamo chiesto ad alcuni dei professionisti che si occupano del tema.

Le soluzioni di riconoscimento facciale in luoghi pubblici sono molto invasive al punto che i garanti privacy europei stanno considerando di vietarle del tutto, a meno che non sia provata l'impossibilità di sostituirle con strumenti meno invasivi. «La stessa presa di posizione è riflessa dalla bozza di regolamento europeo sull'intelligenza artificiale che vieta del tutto soluzioni di riconoscimento biometrico in luoghi pubblici, fatti salvi i casi in cui sia dimostrata la loro necessità», spiega **Giulio Coraggio**, partner di **Dla Piper** e head del dipartimento italiano di Intellectual Property and Technology. «In tale contesto, le sfide più interessanti per gli studi legali come il nostro stanno nel dimostrare la proporzionalità e adeguatezza della scelta di adottare tale tecnologia, l'adeguatezza delle misure tecniche e organizzative adottate e la trasparenza del trattamento rispetto agli individui che sono oggetto del riconoscimento facciale. Inoltre, quando il regolamento europeo sull'intelligenza artificiale sarà realtà si dovrà dimostrare anche la conformità con i requisiti dello stesso».

Per **Chiara Bocchi**, senior associate di **Dentons** «è interessante notare la differenza di percezione della pericolosità del riconoscimento facciale in ambito pubblico e in ambito privato: in ambito pubblico, si tende a individuare soprattutto le criticità trascurando i possibili benefici; al contrario, in ambito privato vengono riconosciuti e apprezzati i benefici del riconoscimento facciale, ignorandone i possibili rischi. Pensiamo soltanto alle modalità di sblocco degli smartphone, o di validazione di transazioni elettroniche: l'abilitazione del riconoscimento facciale viene fatta ormai quasi in automatico, addirittura scegliamo i device anche in base alla loro capacità di funzionare dal punto di vista del riconoscimento facciale e, il più delle volte, senza porci troppe domande sul come i nostri dati biometrici vengono trattati, o su quali misure di sicurezza sono state adottate. È più che giusto che vengano pretese particolari cautele e garanzie per l'utilizzo di sistemi di riconoscimento biometrico in ambito pubblico; altrettanta attenzione dovrebbe, però, essere prestata in ambito privato, a maggior ragione oggi, in un contesto nel quale il valore del dato come corrispettivo di servizi è ormai stato riconosciuto a livello normativo».

Secondo **Jacopo Liguori**, Head of Italian Intellectual Property, Technology & Privacy team di **Withers Studio Legale** «il primo scoglio contro cui si scontra l'impiego di questi avanzati sistemi è di natura giuridica: non esistono infatti a oggi adeguate previsioni normative che consentano ai Comuni o agli enti pubblici di dotarsene. Tale lacuna, che è stata evidenziata anche nel parere del Garante relativo a *Sari Real Time*, riguarda anche altri paesi (come il Regno Unito, la Francia e la Germania), ove le sperimentazioni in tal senso sono state svolte, come già descritto nel report di novembre 2019 dell'Agenzia dell'Unione Europea per i Diritti Fondamentali, senza che fosse possibile individuare una chiara base giuridica per il trattamento. In secondo luogo, diversi studi di letteratura hanno evidenziato la fallibilità di questi sistemi che, verosimilmente a causa dei dati con cui sono stati addestrati, evidenziano margini di errore più alti in soggetti che non siano uomini e che non siano caucasici. Da ciò deriva un evidente rischio di discriminazione, poiché aumentano le probabilità che individui che non rientrano in tali categorie vengano erroneamente identificati con un altro soggetto».

«Si tratta di sistemi in grado di identificare una persona a partire dal suo viso, di generare alert in tempo reale in caso di situazioni anomale, oltre che di fornire servizi accessori», spiega **Paola Finetto**, partner di **Andersen** in Italy. «Questi sistemi di sorveglianza innovativa non sono, tuttavia, ancora pienamente operativi: il Garante per la Protezione dei dati personali e il Parlamento europeo, in particolare, hanno espresso al riguardo molte riserve. Con una risoluzione del 6 ottobre 2021, il Parlamento ha sollecitato la Commissione Ue a istituire un divieto permanente dell'utilizzo di sistemi di sicurezza biometrica, considerato che siffatti sistemi, in quanto anch'essi vulnerabili ed esposti ad attacchi hacker, possono comportare una compromissione ingiustificata delle libertà individuali e del diritto alla protezione dei dati personali. Il diritto alla protezione dei dati personali deve, pertanto, costituire la base per qualunque regolamentazione dell'intelligenza artificiale nel contrasto ai fenomeni criminali».

I comuni di Torino e Udine, adducendo motivi di sicurezza, nei mesi scorsi, hanno deciso l'installazione di sistemi di videosorveglianza con funzioni di riconoscimento facciale suscitando diverse perplessità sulla liceità di tali sistemi alla luce della normativa privacy. «Il Garante Privacy, già con il provvedimento del 26 febbraio 2020, aveva ritenuto illecito il trattamento di dati personali condotto dal Comune di Como mediante telecamere con riconoscimento facciale, non essendoci alcuna norma nazionale che lo giustifichi», spiegano **Bridget Ellison**, partner e **Adriano Garofalo,** associate **De Berti Jacchia.** «Ai sensi dell'art. 7 del dlgs 51/2018, infatti, il trattamento di dati biometrici da parte delle autorità competenti a fini di prevenzione, indagini, accertamento dei reati è lecito solo se strettamente necessario e specificamente previsto da norme europee o nazionali».

Per **Maddalena Valli**, senior manager dello studio legale e tributario ***Legalitax*** «in assenza di una normativa atta a regolare la materia, il rischio è che il riconoscimento facciale, soprattutto se effettuato in contesti pubblici, venga condotto in modo arbitrario e il confronto rimesso alla «discrezionalità» di coloro che saranno chiamati a disporre le immagini fotografiche di confronto. Ciò potrebbe fare insorgere ipotesi di discriminazione e di falsi positivi, anch'essi non regolati sotto il profilo delle conseguenze per gli interessati.

Attesa la delicatezza dei diritti coinvolti, il Comitato europeo e il Garante europeo per la protezione dei dati (rispettivamente Edpb e Edps) sono concordi nell'affermare che queste tecnologie «interferiscono con i diritti e le libertà fondamentali in misura tale da poter mettere in discussione l'essenza di tali diritti e libertà.» Ove, inoltre, le applicazioni di riconoscimento facciale vengano applicate in contesti di massa, afferma il nostro Garante si potrebbe addirittura concretizzare una ipotesi di «sorveglianza universale».

Il riconoscimento facciale usa dati biometrici. «Prima del Gdpr in Italia erano considerati una particolare categoria di dati che, pur non rientrando tra quelli idonei a rivelare informazioni sullo stato di salute (c.d. dati sensibili), erano tuttavia oggetto di particolare tutela poiché relativi a caratteristiche fisiologiche/comportamentali uniche dell'individuo», ricorda **Francesca Gaudino** di **Baker McKenzie.** «Oltre che per la tipologia di dati, i sistemi di riconoscimento facciale destano allarme perché l'uso non regolamentato, in assenza di chiari criteri di limitazione/esclusione e con elastici margini di discrezionalità, può generare conseguenze negative sulla persona. Pensiamo ad esempio a sistemi di sorveglianza predittiva, sistemi che attribuiscono un punteggio sociale alle persone per valutarne l'affidabilità e la meritevolezza, ma anche sistemi di controllo per finalità di sicurezza che finiscono per operare quale sistemi di sorveglianza di massa. Si tratta ovviamente di scenari particolari, in cui le risorse tecnologiche operano in assenza di presidi che ne indirizzino e limitino l'utilizzo, ma si tratta di rischi reali. Rischi riconosciuti in Europa, da Parlamento e tutori istituzionali della privacy (Comitato e garante europeo per la protezione dei dati), che hanno invitato la Commissione a stabilire un divieto generale di ogni utilizzo di sistemi per il riconoscimento biometrico nei luoghi pubblici».

Secondo **Elisabetta Busuito**, partner di **B – Società tra Avvocati,** in generale «gli strumenti di *facial recognition* possono operare sia in real time che in differita: nel primo caso vengono raccolte le immagini di una moltitudine di soggetti ripresi in diretta e confrontate con i dati biometrici presenti nella *watch list* di cui dispone l'Autorità; nel secondo, invece, i dati vengono registrati ed esaminati in un momento successivo, ricercando la corrispondenza tra l'identità di un volto e le immagini presenti in altra banca dati. Nel 2018 il Ministero dell'Interno ha avviato la sperimentazione del Sistema Automatico di Riconoscimento Facciale (Sari), in grado di operare sia in modalità real time che enterprise (quest'ultima si innesta sui dati elaborati nel sistema di identificazione delle impronte). Chiamato a pronunciarsi sulla legittimità del Sari, il Garante Privacy ha reso parere favorevole per il solo Enterprise, non invece al Sari Real Time, stante l'assenza di una base giuridica idonea a regolarlo con le dovute garanzie, anche in ossequio alla Direttiva in materia di trattamento dei dati personali per finalità di law enforcement e alla risoluzione del Parlamento Ue del 6 ottobre 2021».

«Il Garante ha ritenuto che trattamenti di dati biometrici di questa tipologia sono intrusivi perché comportano il rischio di ripercussioni negative sulla vita privata delle persone», spiega **Alessandra Grandoni**, counsel di **Pavia e Ansaldo.** «Per questo motivo il Garante ha bocciato l'iniziativa che avrebbe voluto promuovere il Ministero dell'Interno attraverso il sistema Sari Real Time (parere Garante 25 marzo 2021). Nonostante le molteplici disposizioni del Tulps e del codice di procedura penale, il Garante ha ritenuto che allo stato attuale non vi sia nessuna disposizione del nostro ordinamento giuridico che sia sufficientemente specifica e ponderata da giustificare un simile modello di sorveglianza».

Secondo **Federica Brevetti**, partner di **B&C Legal** «in base al Gdpr, il trattamento di dati biometrici deve essere innanzitutto giustificato da una base normativa (che in Italia non c'è, o almeno non copre le situazioni contemplate dai Comuni), e, aggiunge il Garante, non può essere indiscriminato. Per questa ragione è stato bandito il sistema di videosorveglianza intelligente installato nei giardini della stazione San Giovanni di Como. Quanto a Udine e Torino, i rispettivi impianti, già installati o messi in funzione, sono stati per il momento messi in stand by proprio in seguito ai pareri espressi dal Garante. L'idea che la sicurezza non possa tradursi in sorveglianza di massa è anche alla base della proposta di Regolamento Europeo sull'intelligenza artificiale del 21 aprile 2021. Il testo precisa come i sistemi di identificazione biometrica possano essere usati in spazi pubblici solo per una ricerca mirata (della vittima di un reato, o di soggetti sospettati di particolari crimini), oppure per far fronte ad un pericolo imminente per le persone: i sistemi di riconoscimento facciale sono infatti ancora immaturi, e rischiano di creare distorsioni (si pensi al caso dell'algoritmo di Facebook)».

**Gerardo Giso**, Of Counsel Privacy di **Lexant** rimarca che «ci ha pensato il Garante Privacy a mandare in frantumi il sogno italico di un Grande Fratello peninsulare negando, a più riprese, l'utilizzo dell'intelligenza artificiale per il riconoscimento facciale. Il problema sta nel fatto che si tratta di sistemi non regolamentati, per giunta

ItaliaOggi Sette

diffusione:88589
tiratura:133263



# Manca una normativa univoca sull'uso dei dati biometrici

estremamente invasivi in termini di privacy. Che fare? In attesa del regolamento comunitario, la soluzione dovrebbe essere quella di «educare» soprattutto ai rischi che comportano simili tecnologie che, se mal gestite, potrebbe evolvere in forme di persecuzione «chirurgica». Ricordiamo(ci) che il riconoscimento facciale è stato usato per sopprimere le proteste di Hong Kong tra il 2019 ed il 2020. Non credo che l'opzione fosse nota alla cittadinanza».

Sistemi intrusivi, opachi e fallaci, affidati a enti che di certo non mostrano una particolare sensibilità per i temi connessi alla tutela dei dati personali e che presentano preoccupanti lacune quanto alla sicurezza informatica delle proprie banche dati. Secondo **Alessandro Vasta**, partner **Tonucci & Partners** «quelli che sono a tutti gli effetti veri e propri sistemi di sorveglianza di massa, che comportano la raccolta indiscriminata di dati sensibili, quali sono quelli biometrici, vengono impiegati nelle nostre città senza che i soggetti sorvegliati siano stati debitamente informati, in assenza di un adeguato dibattito pubblico sul tema e in totale spregio alla vigente cornice normativa posta a tutela della riservatezza delle persone fisiche, che ad oggi costituisce l'unico vero presidio a tutela dei cittadini italiani ed europei in tale ambito. L'installazione di un sistema di telecamere dotate di software di riconoscimento facciale, infatti, non solo dovrebbe essere preceduta da una disposizione di legge che ne delimiti l'ambito di utilizzo e preveda adeguate misure a tutela degli interessati, ma innesca tutta una serie di obblighi ulteriori in capo all'ente titolare, inclusa la conduzione di apposita valutazione d'impatto, che, spesso e volentieri, rimangono inadempiuti».

Uno dei profili di maggiore rilevanza è quello relativo alla tutela della privacy in quanto i dati biometrici rientrano nella definizione di dato personale.«Il Garante per la protezione dei dati personali, già nel novembre 2014, aveva emanato delle line guida in cui sono contenuti i principi generali a cui il titolare del trattamento deve attenersi», spiega **Marcello Bana** dello **Studio Legale Bana**. «In estrema sintesi, affinché il trattamento possa considerarsi in conformità con la normativa, dovrà essere accertato: che i dati siano trattai tenendo presenti i presupposti di liceità stabiliti dal Codice, che il sistema biometrico privilegi l'utilizzo di dati anonimi e che i dati rimangano a disposizione per il tempo strettamente necessario, che il trattamento sia effettuato nei limiti dell'informativa (ove richiesta), che siano trattati solo i dati necessari in relazioni alle finalità da perseguire. Il titolare dovrà poi adempiere a tutti gli obblighi a cui è normalmente tenuto per il trattamento dei dati».

Recente anche la sanzione di 200 mila euro del Garante della privacy all'università Bocconi. «Il riconoscimento facciale automatico è l'analisi dell'immagine del volto di un individuo e l'estrazione di un modello digitale di dati, identificativo di un'unica persona, che consente di confrontarlo con caratteristiche di altre immagini digitali», spiega **Lorenzo Mulazzi**, responsabile del Dipartimento compliance di **Eptalex**. «I principali rischi di questa tecnologia sono associabili a esempio alla geolocalizzazione, se utilizzata congiuntamente a sistemi di videosorveglianza. Si pensi all'utilizzo di tale tecnologia da parte delle forze di polizia locale.

Sul tema, veniva pubblicata la bozza di regolamento per l'intelligenza artificiale proposta dalla Commissione europea. Con particolare riguardo al riconoscimento facciale negli spazi pubblici, la bozza precisava che è proibito ma lasciava aperti alcuni scenari di utilizzo con finalità di prevenzione di reati o per la ricerca di persone offese, senza però spiegare le regole di utilizzo da parte delle forze dell'ordine».

«Lo scorso marzo il Garante per la privacy ha reso parere negativo al Ministero dell'Interno sul sistema Sari Real Time», spiega **Edoardo Coia**, Associate dello Studio legale **Eversheds Sutherland**, «ritenendo fosse privo di una base giuridica per il trattamento automatizzato dei dati biometrici per il riconoscimento facciale a fini di sicurezza (le norme richiamate risultavano troppo generiche nelle loro previsioni e dovevano essere attuate da altre normative più specifiche non ancora emanate) e che avrebbe realizzato una forma di sorveglianza indiscriminata/di massa. Infine, il Garante ha recentemente approvato le «body-cam» della Polizia di Stato e dell'Arma dei Carabinieri, purché non si operasse riconoscimento facciale. Emerge quindi che, per evitare di perseguire finalità lecite in modi illeciti e destinare risorse pubbliche per sistemi poi inutilizzabili, occorre che l'implementazione di sistemi di sorveglianza di aree pubbliche sia effettuata previa debita valutazione degli adempimenti secondo la normativa privacy, seppur alla luce della recentissima riforma del Codice Privacy sui trattamenti svolti per eseguire compiti di interesse pubblico o connessi all'esercizio di pubblici poteri».

L'assenza di una disciplina legislativa specifica che regoli l'utilizzo di tale tecnologia, le problematiche in materia di proporzionalità e trasparenza del trattamento nonché i rischi di profilazione e discriminazione connessi al suo utilizzo rendono particolarmente controverso l'uso del riconoscimento facciale specialmente in luoghi pubblici. «L'utilizzo di sistemi di riconoscimento facciale potrebbe presto essere regolato a livello europeo», afferma **Laura Baldisserra** di **Jones Day.** «È infatti in corso di approvazione un Regolamento Europeo in materia di intelligenza artificiale che disciplina anche l'utilizzo di tali tecnologie. L'attuale testo della proposta vieta l'utilizzo di sistemi di identificazione biometrica remota in tempo reale in spazi aperti al pubblico per attività di contrasto, salvo che l'utilizzo di tali sistemi sia strettamente necessario per la ricerca di potenziali vittime di reato, la prevenzione di una minaccia specifica o la ricerca di un autore di specifiche tipologie di reato».

L'IA è adottata da diversi comuni

Le Linee Guida sul riconoscimento facciale del Consiglio d'Europa hanno affidato alla legge nazionale di ciascun Stato aderente il compito di specificare le finalità del trattamento, i parametri di affidabilità dell'algoritmo, il periodo di conservazione, oltre che adeguate procedure volte a garantire i diritti degli interessati. «A livello italiano», spiega **Marco Agostini** di **Gr Legal**, «si segnala il parere del Garante sul sistema di videosorveglianza Sari Real Time del 25 marzo 2021, oggetto di una richiesta di parere preventivo da parte del Ministero dell'Interno. Questa tecnologia prevede la possibilità di paragonare in tempo reale le immagini di persone fisiche raccolte da una telecamera, con quelle di soggetti conservate negli archivi del Ministero, per il perseguimento di finalità di pubblica sicurezza. In questo parere il Garante ha evidenziato: i) che non sussiste, a oggi, una base giuridica idonea a legittimare il confronto in tempo reale delle immagini raccolte da un impianto in funzione con quelle presenti nei data base delle forze di polizia; che un intervento del legislatore dovrebbe dettagliare precisamente le fattispecie in in cui l'uso di tali apparati è lecito e i criteri per individuare i soggetti che possono essere inseriti nelle c.d. «watch-list». Fondamentale, dunque, nella prospettiva del Garante, è predeterminare per legge i casi in cui tali trattamenti sono possibili, in modo da sottrarli alla discrezionalità dell'amministrazione e dell'operatore addetto all'utilizzo del sistema».

La non accettabilità di un simile sistema è comunque rinvenibile da una breve analisi delle posizioni delle autorità privacy sul tema. «Sul punto è intervenuto innanzitutto il Comitato Europeo per la Protezione dei dati personali (Edpb), che nelle Linee Guida n°3/2019 si è soffermato sul tema del riconoscimento facciale nei sistemi di videosorveglianza, sottolineando che «l'uso di dati biometrici, in particolare il riconoscimento facciale, comporta maggiori rischi per i diritti degli interessati» e che «i titolari del trattamento dovrebbero considerare mezzi meno intrusivi per raggiungere il legittimo scopo del rispettivo trattamento», ha ricordato **Marco Sebastiano Accorrà** di **Msà Law Firm.** «Inoltre, anche il nostro Garante della Privacy, chiamato proprio a valutare il sopra citato caso di Como, ha ritenuto con provvedimento del 26 febbraio 2020 che la raccolta di dati biometrici (categoria nella quale rientrano le caratteristiche del viso) possa effettuarsi «solo in presenza di un'idonea previsione normativa, che al momento non pare rinvenibile».

E ancora, sempre il Garante della Privacy ha dato parere non favorevole sull'utilizzo del sistema Sari Real Time del Ministero dell'interno che avrebbe consentito attraverso una serie di telecamere di analizzare in tempo reale i volti dei soggetti ripresi, confrontandoli con una banca dati predefinita (denominata "watch-list"), che può contenere fino a 10 mila volti. Il sistema, anche in questo caso, è stato definito «privo di una base giuridica che legittimi il trattamento». Insomma, si può concludere che, ad oggi, un sistema come quello in esame sarebbe da considerarsi a tutti gli effetti illegale».

Per **Giovanna Boschetti**, associata studio **Cba** «l'implementazione di tecnologie di riconoscimento facciale comporta, in sostanza, l'applicazione di software biometrici in grado di verificare in modo univoco l'identità di una persona fisica. Gli aspetti più importanti lato privacy e conformità al Gdpr attengono alle misure preventive ed alla valutazione del rischio, alla base giuridica del trattamento (tenuto conto del bilanciamento degli interessi e del principio di mitizzazione), al trasferimento di dati all'estero (considerato che le società più rilevanti nel settore cloud sono extra Ue), alla conservazione dei dati ed alle ipotesi di violazioni di dati (c.d. data breach), che coinvolgono sia gli aspetti tecnici di sicurezza sia quelli organizzativi di gestione dell'evento di data breach.

È, quindi, indispensabile che tutti gli stakeholders si attivino sin d'ora al fine di completare il percorso di cultura e formazione nell'uso dei sistemi di sorveglianza biometrica lato Gdpr ed essere pronti ad implementare tutti gli inerenti processi aziendali».

L'avvio sperimentale di progetti locali che impiegano tecnologie di riconoscimento facciale intelligente presenta diversi profili di criticità. «Le tecnologie non mature di riconoscimento facciale espongono anche al rischio concreto di violare gli obblighi legali di non discriminazione in particolare in relazione all'origine nazionale ed etnica, al sesso ed al genere, giacché è dimostrata una diversa capacità di riconoscimenti dei maschi bianchi rispetto ad altre classi di persone», spiega **Mario Di Carlo**, partner dello **studio legale Ristuccia Tufarelli & Partners** dove si occupa di diritto d'impresa e diritti umani, presidente di Edge e socio di Avvocatura per i diritti LGBTI – Rete Lenford, «Ciò comporterebbe pacificamente una violazione quanto meno dell'art. 43 del decreto legislativo n. 286/1998, del dlgs. n. 215/2003 e dell'articolo 55-ter del Codice delle pari opportunità, sotto forma di discriminazione diretta o indiretta a seconda dei casi».

Per **Luca Tufarelli**, partner e founder dello Studio legale Ristuccia Tufarelli & Partners, «anche quando si riuscisse ad individuare un'idonea base giuridica del trattamento, l'Autorità evidenzia la necessità di porre degli argini anche alla tecnica di riconoscimento che si intende impiegare, con specifico riferimento ai criteri per l'individuazione dei soggetti che possono essere inseriti nella «watch-list» o quantomeno per determinare i casi in cui può il sistema può essere utilizzato. Il tutto, nell'ottica di un equo bilanciamento di interessi contrapposti meritevoli di tutela, quali la privacy dei cittadini, da un lato, e le esigenze di sicurezza, dall'altro».

Per **Pietro Montella**, founding partner **Montella Law** «il rischio, come più volte paventato, è una pericolosa evoluzione della natura stessa dell'attività di sorveglianza, che segnerebbe un passaggio dalla sorveglianza mirata di alcuni individui alla possibilità di sorveglianza di massa.

È proprio a causa della loro forte interferenza con la vita privata delle persone che la normativa in materia di privacy stabilisce rigorose cautele per i trattamenti di dati biometrici, i quali devono trovare giustificazione in una adeguata base normativa, senza tralasciare il rispetto dei principi contemplati dal Gdpr, tra i quali figura la minimizzazione del dato».

Ma può il riconoscimento facciale essere oggi utilizzato come prova nel processo? «Certamente no, dal momento che, per i sistemi esistenti, non è ancora possibile dimostrare né la «scientificità» del metodo applicato, nè l'affidabilità dello strumento in concreto impiegato», conclude **Enrico Di Fiorino**, partner di **Fornari e Associati**, «Al più, quindi, il risultato potrà essere utilizzato come spunto investigativo. In aggiunta, è sempre più diffusa la consapevolezza della drammatica invasività di tali sistemi e della enorme quantità di dati raccolti, in ipotesi utilizzabili per finalità illecite o comunque abusive».

*Supplemento a cura*
di Roberto Miliacca
rmiliacca@italiaoggi.it
e Gianni Macheda
gmacheda@italiaoggi.it