Alla scoperta dell'intelligence privata

FEDERPOL MAG

investigazioni | informazioni | sicurezza

LA SCENA DEL CRIMINE
La strage di Erba
di nuovo sotto la lente

L'APPROFONDIMENTO
Giustizia predittiva:
la sfida degli algoritmi

INVESTIGAZIONI
Tutto quello che c'è da sapere
per operare all'estero

L'INTERVISTA
Come prevenire e contrastare
la criminalità informatica

Avvocati e investigatori: una collaborazione che si concretizza

FW Communication

www.federpol.it

ANNO III | NUMERO 6

L'APP dei Soci Federpol

DISPONIBILE PER IOS E ANDROID

LAMSERVICE

Informazioni & Servizi per il mondo degli affari

Tutta la documentazione che cerchi è a portata di click

Tutti i Vantaggi di LAM Service in una sola Card!

Servizio Camerale
Info Commerciali
Info Pre-Fido e Post-Fido

WWW.LAMSERVICE.IT

Oltre 2.000.000 di Richieste Evase

distributore ufficiale di "InfoCamere" | Telemaco | Banca Dati OnLine tutto in un click

Lam Service Srl
Sede Legale: Via Besana, 10 - 20122 Milano
Centro Operativo: Via Toscana, 12 Int. D1/11 - 20060 Vignate (MI)
Tel. 029587847 - Email: info@lamservice.it - Web: www.lamservice.it

FAI CRESCERE LA TUA AZIENDA

Attraverso l'Avviso a Sportello 2/2022 promuoviamo, in tempi veloci e sicuri, l'implementazione delle conoscenze necessarie alle imprese.
Una risposta concreta alle reali necessità formative delle aziende aderenti a Fondo Formazienda.

GRUPPO rts REAL TRAINING SOLUTIONS

FORMAzienda®
FONDO PARITETICO INTERPROFESSIONALE NAZIONALE PER LA FORMAZIONE CONTINUA

Numero Verde 800-010333

www.rts-srl.it • info@rts-srl.it
P.zza M. Ruini n. 29/A 43126 Parma (PR)

SOMMARIO

Numero 6 | 2023

DAL 1957 PUNTO DI RIFERIMENTO PER I PROFESSIONISTI DELL'INVESTIGAZIONE,
DELL'INFORMAZIONE COMMERCIALE E DELLA SICUREZZA

WWW.FEDERPOL.IT

TUTELA I TUOI INTERESSI
ED ENTRA A FAR PARTE DELLA SQUADRA FEDERPOL

WWW.FEDERPOL.IT

FEDERPOL: VIA MILANO, 51 - 00184 ROMA TEL. +39 06 37518900 EMAIL: FEDERPOL@FEDERPOL.IT

di Luciano Tommaso Ponzi
Presidente Federpol

Elevare la consapevolezza: il fondamentale ruolo della professionalità nell'investigazione

Nel mondo dell'investigazione, la professionalità è una qualità fondamentale che non solo definisce il successo di un professionista, ma influenza anche l'integrità e la fiducia dell'intero settore.
La professionalità non è semplicemente un insieme di regole o protocolli da seguire, ma una filosofia che permea ogni aspetto del lavoro investigativo. Essa inizia con un impegno profondo per l'onestà, l'integrità e la dedizione al perseguimento della verità; un investigatore professionale non cerca solo di risolvere casi, ma di farlo nel modo più giusto possibile, rispettando sempre i diritti e la dignità delle persone coinvolte. Essere un professionista nell'ambito investigativo richiede una costante ricerca di conoscenza e abilità. Gli investigatori professionisti investono tempo ed energie per aggiornarsi sulle ultime tecniche investigative, leggi e tecnologie e questo impegno alla formazione continua consente di offrire ai clienti un servizio di alta qualità e di mantenere uno standard elevato nell'industria.

Un aspetto spesso trascurato ma determinante è la capacità di comunicare in modo chiaro ed efficace. Gli investigatori devono essere in grado di trasmettere informazioni complesse in forma comprensibile ai clienti, ai colleghi e, quando necessario, alle autorità competenti. Questa abilità non solo facilita il processo investigativo, ma contribuisce anche a rafforzare la fiducia e la reputazione della professione. Una parte cruciale è la gestione delle aspettative dei clienti. Gli investigatori professionisti sono trasparenti rispetto ai risultati e alle tempistiche delle indagini. Questa comunicazione aperta e onesta instaura fiducia e riduce il rischio di delusioni. I clienti che comprendono le limitazioni dell'investigazione sono più propensi a essere soddisfatti dei risultati ottenuti.

La professionalità nell'ambito investigativo si manifesta anche attraverso il rispetto per la riservatezza delle informazioni. Gli investigatori hanno accesso a dati sensibili e personali, e il loro dovere è proteggerli con la massima cura; la mancanza di riservatezza può compromettere l'efficacia del lavoro investigativo e danneggiare la reputazione del professionista.
Essere professionisti significa anche assumersi la responsabilità sociale. Gli investigatori contribuiscono alla giustizia e alla sicurezza della società, e quindi devono operare in maniera etica e responsabile. La professionalità è il fondamento su cui si basa l'intero settore investigativo ed è ciò che distingue i veri professionisti e garantisce la credibilità e l'efficacia del lavoro svolto.

Gli investigatori consapevoli del loro ruolo sanno che il loro lavoro va oltre la semplice risoluzione di casi; esso promuove la giustizia e il rispetto per l'individuo. La professionalità è la chiave per aprire le porte della verità e mantenere alto il prestigio dell'investigazione nel mondo moderno. In un'epoca in cui le sfide etiche e legali sono sempre più complesse, gli investigatori professionisti devono essere ancorati ai principi etici. La professionalità richiede il rispetto rigoroso dei confini legali e morali, garantendo che l'indagine non solo sia condotta scrupolosamente, ma anche in modo giusto e rispettoso. L'equilibrio tra la necessità di risolvere i casi e il rispetto delle leggi e dei diritti umani è una sfida continua, che gli investigatori professionisti abbracciano.

L'investigazione è un'arte, una scienza e una missione. E in ogni aspetto di questa disciplina, la professionalità è la chiave per sbloccare il potenziale più alto e per garantire un futuro migliore per l'intera professione.

Congresso Federpol 2023: avvocati e investigatori insieme per la verità

Il 66° Congresso Nazionale Federpol si è tenuto l'11 e il 12 maggio a Giardini Naxos in Sicilia. Il patto di collaborazione tra avvocati e investigatori privati è stato il tema al centro delle due giornate che hanno riunito i protagonisti delle investigazioni e della sicurezza.

di Laura Reggiani

Un gruppo di investigatori, con al centro il presidente Ponzi, al 66° Congresso Nazionale Federpol a Giardini Naxos

Importante la presenza e il contributo delle investigatrici al 66° Congresso Nazionale della Federazione

Gli sponsor che hanno reso possibile l'organizzazione del 66° Congressso Nazionale Federpol

Il patto di collaborazione tra avvocati e investigatori privati, tema principale del **66° Congresso Nazionale Federpol**, è stato sancito all'inizio dell'anno da un importante protocollo d'intesa firmato tra la Federazione e la **Scuola Superiore dell'Avvocatura**. Il protocollo prevede la realizzazione di azioni comuni volte a promuovere e incentivare iniziative di informazione sulla figura dell'investigatore privato, nonché lo sviluppo di percorsi formativi diretti ad avvocati e investigatori privati muniti di licenza. In questo modo, si mira a creare una collaborazione più stretta tra le due categorie professionali, che potrà portare benefici reciproci e garantire una maggiore efficacia nelle attività investigative. E proprio in quest'ottica è stato organizzato anche il Congresso che, prendendo spunto dal tema centrale *"Avvocato e*

investigatore privato, due professionisti uniti nella ricerca della verità", ha visto protagonisti numerosi relatori che si sono confrontati sui principali temi di interesse per la categoria. I lavori si sono tenuti l'11 e il 12 maggio a Giardini Naxos, presso i suggestivi spazi di **UNAHotels Naxos Beach Sicilia**, e si sono strutturati con diversi appuntamenti, tra cui un corso di aggiornamento professionale e l'assemblea generale dei soci nella giornata di giovedì 11 maggio; i lavori del congresso e la cena di gala venerdì 12 maggio. L'evento ha visto la partecipazione di circa 200 addetti del settore delle investigazioni private, confermandosi come momento importante e occasione di confronto e di aggiornamento per gli investigatori e gli operatori della sicurezza privata, a dimostrazione dell'impegno della Federazione nell'affermare e tutelare la professionalità della categoria.

Risultati e obiettivi della Federazione

I lavori sono stati aperti dalla relazione del presidente **Luciano Tommaso Ponzi**, che ha tracciato un bilancio dell'attività svolta dalla Federazione e dei risultati conseguiti. *"La nostra"*, ha detto Ponzi, *"è una lunga storia, cominciata nel 1957. Consentitemi, anzitutto, di ricordare chi ci ha preceduto e oggi non c'è più, cui va tutta la nostra riconoscenza per averci trasmesso quell'orgoglio di appartenenza che da sempre caratterizza noi investigatori privati"*. Ponzi ha sottolineato nella sua relazione anche di avere raggiunto *"l'ennesimo risultato importante per la categoria, ovvero la firma di un protocollo di intesa con la Scuola Superiore dell'Avvocatura, fondazione del Consiglio Nazionale Forense"*. Come ha spiegato il presidente, si tratta di *"un protocollo importantissimo non solo per i suoi contenuti, ma anche perché segna una tappa fondamentale nel percorso di legittimazione formale della nostra professione, che non si riconosce più nei falsi miti e negli stereotipi del passato, ma piuttosto rivendica, con orgoglio, un profilo talmente alto da poter favorire nella strada impervia diretta alla verità processuale, l'effettività del diritto di difesa"*. Il presidente di Federpol ha poi ricordato gli altri traguardi, come l'accordo per la certificazione universitaria assieme al primo corso di laurea nelle **Università "Tor Vergata"** e **Unimercatorum** di Roma, la firma di un nuovo contratto collettivo nazionale per la categoria presso il **Cnel** e il tanto atteso riconoscimento del tesserino professionale, in via di realizzazione presso il Poligrafico e Zecca dello Stato. Il presidente Ponzi ha concluso con un appello all'unità: *"Come in tutte le migliori famiglie può capitare di avere incomprensioni, soprattutto quando alla base c'è, come nel nostro caso, una grande passione. Eppure, in ognuno di noi non è mai mancato quell'orgoglio di appartenenza che ci ha sempre permesso di smussare angoli e superare divisioni"*.

Il sostegno alla categoria

Molti gli interventi degli oltre 20 relatori che hanno attirato l'attenzione dei partecipanti. Dopo i saluti istituzionali del sindaco di Giardini Naxos **Giorgio Stracuzzi** e dei portavoce della Polizia di Taormina, del vice presidente area Sud di Federpol **Marco Gallo** e della dottoressa **Milene Sicca** del Comitato studi legislativi, si sono susseguiti una serie di speech che hanno portato contenuti di interesse per gli investigatori privati.
Sul versante politico vanno segnalati gli interventi del senatore **Andrea De Priamo** e dall'onorevole **Bernadette Grasso**. *"C'è la volontà di sostenere la categoria degli investigatori privati, che sta facendo tanto per modernizzarsi e affrontare l'evoluzione della digitalizzazione, che amplia l'attività di questo settore"*, ha affermato il senatore Andrea De Priamo, membro della prima commissione permanente Affari istituzionali. *"Ho presentato una interrogazione, anche alla luce di una iniziativa di Federpol, per chiedere al Ministero degli Interni la possibilità di accesso, così come altre categorie, all'Anagrafe nazionale delle persone residenti, uno strumento penso fondamentale, nei limiti che prevede la legge, per consentire agli investigatori privati di operare a 360 gradi e di fare bene il loro lavoro. Sono fiducioso sul buon esito della mia istanza"*, ha concluso.
L'utilità della collaborazione con gli investigatori privati è stata sottolineata anche dall'onorevole Bernadette Grasso, vicepresidente della commissione Antimafia della Regione siciliana all'Ars. *"La Federazione"*, ha detto la Grasso, *"è un sodalizio antichissimo che con accordi recenti fortifica il ruolo dell'investigatore. Adesso si hanno tecniche investigative*

Da sinistra, in alto:
Luciano Tommaso Ponzi,
Marco Gallo,
Miléne Sicca,
Andrea De Priamo,
Berlino Tazza,
Matteo Pariscenti,
Vito Campo,
Gabriele Faggioli,
Eraldo Stefani,
Francesco Sardi de Letto,
Marcello La Bella

SCOPRI IL MONDO FEDERPOL

WWW.FEDERPOL.IT

FEDERPOL: VIA MILANO, 51 - 00184 ROMA TEL. +39 06 37518900 EMAIL: FEDERPOL@FEDERPOL.IT

che necessitano di ulteriore professionalità. È importante il loro apporto anche nel settore ambientale, dove gli investigatori privati potrebbero dare il loro contributo".

Sicurezza dei dati e privacy

Dal punto di vista tecnologico è stato di particolare rilievo l'intervento di **Gabriele Faggioli**, presidente del **Clusit**, l'associazione italiana per la sicurezza informatica. *"Sono stati circa 2.500 cyberattacchi di pubblico dominio in Italia solo nel 2022"*, ha commentato Faggioli presentando i dati dell'ultimo rapporto. *"Abbiamo registrato un picco di attacchi in corrispondenza dell'inizio delle ostilità tra Russia e Ucraina, avvenuto tra febbraio e marzo, attacchi che non hanno toccato comunque l'Italia, anche perché non erano intenzionati ad andare a fondo. Nella maggior parte dei casi l'85% degli attacchi è stato effettuato da criminali a esclusivo scopo di lucro"*.
Sul punto è intervenuto anche l'avvocato **Guido Scorza**, componente dell'Autorità Garante per la protezione dei dati, che ha evidenziato le due anime del diritto alla privacy: quella della riservatezza personale e quella del diritto all'identità personale e del loro impatto sulla vita delle persone. Infine, sempre in tema digitale, il dottor **Marcello La Bella**, dirigente del Centro Operativo per la Sicurezza Cibernetica e della Polizia Postale della Sicilia Orientale (ndr: trovate l'intervista nelle pagine seguenti) ha parlato delle indagini svolte sulla rete, un mondo reale che non ha confini geografici e in cui imperversano reati che spaziano dal revenge porn al sexting, dagli attacchi alle infrastrutture critiche alle truffe online, fino alla pedopornografia.

Premiazioni e Galà

Il pomeriggio è poi proseguito con la premiazione delle tesi di laurea, che ha visto classificarsi in prima posizione **Fabrizio Farris** dell'**Università La Sapienza** (ndr: l'estratto della sua tesi è nelle pagine seguenti), **Letizia Berardi** dell'**Università di Perugia** al secondo posto e **Francesco Guardagno** al terzo posto.
Infine, la giornata si è conclusa con la consueta cena di gala, con circa 200 ospiti presenti, allietata da musica dal vivo, che poi è proseguita nel **Federpol Party** all'insegna della musica degli Anni 70 e 80.

Un momento musicale nella serata di giovedì 11 maggio ha dato il via al 66° Congresso Nazionale della Federazione

La cena di gala di venerdì 12 maggio ha chiuso i lavori del 66° Congresso Federpol e riunito oltre 200 persone

I festeggiamenti sono terminati con il consueto taglio della torta

La strage di Erba e la traccia di sangue

Tra le motivazioni portate dal procuratore Tarfusser per la richiesta di revisione della sentenza di condanna nei confronti di Rosa Bazzi e Olindo Romano c'è quella che la traccia di sangue trovata possa "con ogni probabilità non provenire dal battitacco dell'autovettura di Olindo". L'attenta lettura degli atti processuali sembra però dimostrare tutt'altro.

di Luciano Garofano

Il 26 marzo scorso il Sostituto Procuratore Generale di Milano, dottor **Cuno Tarfusser** con un documento di 58 pagine ha inoltrato al Presidente della Corte di Appello di Brescia una richiesta di revisione della sentenza di condanna nei confronti dei coniugi **Rosa Bazzi** e **Olindo Romano**.
La presunta innocenza di Rosa e Olindo è stata da sempre sostenuta dalla trasmissione "Le Iene" e ha già registrato due richieste di revisione che sono state ritenute inammissibili. Finora, però, Rosa e Olindo, che il 3 maggio 2011 sono stati condannati all'ergastolo, rimangono gli autori materiali della strage di Erba.

La scena del crimine

Via Diaz è una viuzza di Erba, una cittadina della provincia di Como, adagiata ai piedi delle Prealpi lombarde. Al numero 25 si trova una tipica casa colonica, costruita intorno a una corte, ora completamente circondata dall'abitato. La piazza del mercato dista solo 50 metri. Sul lato sud del cortile si trova una caratteristica casa di ringhiera lombarda, su quello a nord-ovest ci sono un fienile riconvertito in garage e un piccolo appartamento, e l'edificio principale conosciuto nel dialetto locale come *"Ca' del Giaz"*, con abitazioni al pianterreno, al primo piano e

nella mansarda. Lo spazio tra l'ex fienile e la palazzina principale è stato trasformato in un garage il cui tetto è diventato una terrazza.
Glauco Bartesaghi è un uomo atletico che ha superato la quarantina. Abita in uno degli appartamenti sul lato sud della corte. Si mantiene in forma grazie al suo lavoro di volontario dei Vigili del Fuoco. La sera dell'11 dicembre 2006, intorno alle 20,20, viene chiamato da un vicino, **Vittorio Ballabio**, perché sta uscendo del fumo dall'appartamento di **Raffaella Castagna** e di suo marito **Azouz Marzouk**, al primo piano, sul lato nord del cortile. Bartesaghi avvisa sua moglie di telefonare subito al 115 e, insieme a Ballabio, percorre velocemente il cortile. Prima di riuscire a entrare sono costretti a spostare un'auto che blocca la porta d'accesso. Quando giungono al primo piano s'imbattono in una scena raccapricciante: Raffaella Castagna giace in una pozza di sangue con gli abiti in fiamme, appena dentro l'ingresso di casa sua. La porta era aperta. Bartesaghi trascina la giovane sul pianerottolo per toglierla dalle fiamme e spegnere quelle che la avvolgevano. Il fuoco è già diffuso in tutte le stanze e l'unico estintore che Ballabio ha portato con sé non appare sufficiente. I due devono abbandonare subito l'abitazione. Sul pianerottolo, all'ingresso dell'appartamento dei Marzouk, giace anche **Mario Frigerio**, inquilino del secondo piano, anch'egli in una pozza di sangue; non riesce a parlare ma indica in modo frenetico in direzione della mansarda, dove abita con la moglie **Valeria Cherubini**. I due uomini la sentono gridare. Quando Bartesaghi apre una finestra della tromba delle scale, le volute di fumo provenienti dall'appartamento in fiamme fluttuano verso l'interno dello stabile, invadendo il pianerottolo, e i due volontari sono costretti ad abbandonare l'edificio trascinando con sé Frigerio: secondo Bartesaghi sono passati circa cinque minuti da quando sono arrivati lì.
La telefonata ai vigili del fuoco viene inoltrata alla squadra del posto alle 20,29 e alle 20,38 le autopompe iniziano le operazioni. Il Comando dei pompieri in realtà dista appena cinquecento metri dalla Ca' del Giaz, ma la chiamata di emergenza ha dovuto passare per il centralino del Comando provinciale di Como. Sul posto giungono anche i Carabinieri di Erba e il loro comandante, il luogotenente **Luciano Gallorini**.
Una volta sedato l'incendio, i soccorritori riescono finalmente a entrare in casa e, anche loro, non ce la fanno a trattenere l'orrore. Raffaella Castagna giace dove l'aveva lasciata Glauco Bartesaghi, sul pianerottolo, mentre all'interno dell'appartamento, sua madre, Paola Galli, viene trovata distesa nel corridoio, in posizione prona: è stata accoltellata ripetutamente e colpita alla testa. Nel salotto, riverso sul divano, c'è anche il figlioletto di Raffaella, Youssef, di appena 2 anni, sgozzato. Al secondo piano, trovano invece Valeria Cherubini genuflessa accanto alla finestra con ferite multiple al capo e una alla gola, inferta probabilmente da una lama che era penetrata fino in bocca e le aveva tranciato la lingua.

I dubbi sulla responsabilità di Rosa e Olindo

Nella sua articolata relazione, il dottor Tarfusser avanza seri dubbi su quelli che sono da considerare i pilastri di questo drammatico caso:

1 | il riconoscimento da parte di Mario Frigerio di Olindo Romano quale suo aggressore;
2 | le confessioni di Rosa Bazzi e di Olindo Romano;
3 | la macchia di sangue rinvenuta sul battitacco dell'auto di Olindo Romano appartenente in vita a Valeria Cherubini.

Non entrerò nel merito dei primi due, in quanto esulano dalle mie competenze. È certo, però e questo va detto, che appare assai strano dover ammettere che quella dei due coniugi sia stata una confessione del tutto inventata, vista la ricchezza dei particolari e la precisione con

Il cortile di via Diaz numero 25, a Erba, cittadina in provincia di Como, dove vivevano Raffaella Castagna e la sua famiglia.

Particolare del battitacco dell'auto di Olindo Romano.

cui Olindo e Rosa hanno raccontato l'intera vicenda. Ne è possibile pensare che tale dovizia di elementi sia stata il frutto della mera visione delle fotografie che gli sarebbero state mostrate nel corso dell'interrogatorio.
Pari perplessità devono essere mosse sulla non genuinità delle dichiarazioni di Mario Frigerio, o meglio, sulle pressioni che gli sarebbero state fatte per *"estorcergli"* il nome di Olindo Romano. E non soltanto perché questo può essere fugato dalla attenta valutazione di tutti i video che documentano gli incontri di Frigerio con la polizia giudiziaria e con i magistrati, ma anche e soprattutto per una semplice valutazione di logica: quale interesse recondito poteva avere Frigerio, una volta convocato in dibattimento, nel confermare con fermezza che chi l'aveva accoltellato fosse proprio Olindo?

I coniugi Rosa Bazzi e Olindo Romano, condannati all'ergastolo nel 2011.

Le tracce di sangue e il loro trattamento

Ma veniamo al terzo aspetto, quello che riguarda la famosa macchia di sangue presente sul battitacco dell'autovettura dei due coniugi. Ciò che il dottor Tarfusser ipotizza è molto grave, vale a dire che quella traccia *"con ogni probabilità non provenga dal battitacco dell'autovettura di Olindo Romano"*. L'attenta lettura degli Atti, però, sembra dimostrare tutt'altro. È necessario rileggere le motivazioni della sentenza di primo grado per rendersi conto che, diversamente da quanto sostenuto dal Procuratore Generale, il tema fu ampiamente esplorato nel corso del dibattimento. È il brigadiere **Carlo Fadda** che, all'udienza dell'11 febbraio del 2008, spiega nel dettaglio le operazioni compiute: la ricerca di tracce biologiche all'interno dell'autovettura Seat Arosa, viene effettuata verso le ore 23 del 26 dicembre 2006 alla presenza del proprietario Olindo Romano, ispezionando dapprima l'autovettura con le luci forensi e sottoponendola immediatamente dopo alla nebulizzazione con il Luminol - un composto chimico che reagendo con l'emoglobina produce una debole luce bluastra rilevabile soltanto se il trattamento viene eseguito al buio - poiché l'esame con le luci non aveva permesso di individuare tracce sospette. Il trattamento con il Luminol, precisa Fadda, fornisce un esito positivo su quattro aree dell'autovettura:

1 | sul battitacco lato conducente;
2 | sulla portiera sinistra nell'area compresa tra la maniglia e la griglia del diffusore sonoro;
3 | sulla manopola che consente la regolazione dell'altezza del sedile del conducente;
4 | sulla parte sinistra del cuscino di seduta del sedile del passeggero.

E poiché c'è il rischio che esse si disperdano, vengono campionate immediatamente, trasferendole su porzioni di carta da filtro sterile (una specie di carta assorbente), procedendo soltanto dopo a fotografare le quattro aeree, sebbene sarebbe stato più corretto documentare la positività al Luminol. Così campionate, le quattro tracce vengono fatte asciugare e dopo averle confezionate in altrettante buste di carta con l'indicazione del loro contenuto, tre giorni dopo, vengono consegnate al dottor **Carlo Previderé**, genetista forense

Che la traccia di sangue possa essere il frutto di una contaminazione operata dai Carabinieri che precedentemente erano intervenuti sulla scena del quadruplice omicidio è da escludere, poiché coloro che nell'immediatezza perquisirono l'autovettura di Olindo Romano non erano stati sulla scena del crimine, ed è da scartare che possano essere stati gli stessi coniugi a trasportare sulla loro auto tracce ematiche, poiché non gli fu permesso alcun accesso in quell'area.

dell'Università di Pavia che, dopo averne riscontrato l'integrità e il contenuto le sottopone alle analisi bio-genetiche. Soltanto una, però, risulterà appartenere alla natura ematica, quella prelevata dal *"battitacco del lato conducente"* che, sottoposta all'analisi del Dna, dimostrerà di appartenere a Valeria Cherubini. Che quella traccia possa essere il frutto di una contaminazione operata dai Carabinieri che precedentemente erano intervenuti sulla scena del quadruplice omicidio è da escludere, poiché coloro che nell'immediatezza perquisirono l'autovettura del Romano non erano stati sulla scena del crimine ed è da scartare che possano essere stati gli stessi coniugi a trasportare sulla loro auto tracce ematiche, poiché non gli fu permesso alcun accesso in quell'area. Che quella traccia non fosse rilevabile a occhio nudo, tanto da suggerire il ricorso al Luminol, non costituisce, inoltre, un dato contrastante rispetto al successo dell'analisi genetica: si può ricavare una discreta quantità di Dna (dato tecnico cui si riferiva il dottor Previderè quando fu esaminato in dibattimento) e quindi un profilo utile per l'identificazione personale, anche da tracce di sangue invisibili. Se, peraltro, quel Dna fosse derivato da una contaminazione, il profilo ricavato da Previderè avrebbe mostrato la presenza di tracce incomplete di Dna (alleli) riferibili a tutte le vittime o, addirittura, una quantità inidonea per le successive analisi genetiche, in considerazione della diluizione causata dai Vigili del Fuoco per domare l'incendio. E, contrariamente a quanto sospettato dal dottor Tarfusser, non può nemmeno ipotizzarsi una diversa possibilità di contaminazione o addirittura lo scambio tra i reperti, poiché le quattro tracce repertate dall'autovettura non sono mai venute in contatto con gli abiti della Cherubini, che furono repertati in sede autoptica e trasmessi dai Carabinieri al dottor Previderè in contenitori e tempi diversi.

Non ho elementi per dire se la richiesta del dottor Tarfusser avrà un seguito e se questa potrà avere degli effetti su una possibile revisione del processo. È però doveroso sottolineare che i dubbi e le perplessità sollevate dal Procuratore Generale, seppur legittimi, hanno già avuto esaurienti risposte nel corso dei tre gradi di giudizio che hanno condannato Rosa e Olindo in via definitiva.

Chi è Luciano Garofano

Laureatosi nel 1976 in Biologia all'Università degli Studi di Roma La Sapienza, **Luciano Garofano** si è successivamente specializzato all'Università degli Studi di Napoli Federico II in tossicologia forense, nel 1993. Nel 1978 si arruola nell'Arma dei Carabinieri e fino al 1988 è al comando della Sezione Chimico-Biologica del Centro Carabinieri Investigazioni Scientifiche di Roma. Dal 1988 al 1995 è comandante della Sezione Biologia dello stesso centro. Dal 1995 fino al 2009 è stato comandante del **Ris di Parma**, dove si è occupato di vari casi di cronaca nera tra i quali la strage di Erba, il serial killer Bilancia, il delitto di Novi Ligure, il caso Cogne e il delitto di Garlasco. È docente universitario e di master per le materie Criminalistica e Tecniche del Sopralluogo, è autore di numerose pubblicazioni scientifiche nazionali e internazionali e di diversi libri su casi di interesse nazionale. In congedo dal 2010 dall'Arma dei Carabinieri con il grado di Generale, è attualmente libero professionista e consulente.

Breve guida pratica al "colloquio investigativo"

La testimonianza, ovvero la dichiarazione resa da un soggetto informato sui fatti, non costituisce solo un mezzo per comprendere la dinamica dei fatti, ma rappresenta una prova molto considerata sia nel processo civile che in quello penale.

di Ugo Terracciano

Vuoi trovare il responsabile? Allora cercane le tracce. Non c'è bisogno di Sherlock Holmes per capirlo: è un meccanismo causa-effetto che muove ogni accadimento bello o brutto da sempre nel mondo: il cosiddetto rapporto causale, nel diritto.
E poi, non dimentichiamolo, la traccia è un concetto che sta all'origine stessa del termine *"investigatore"* (dal latino *vestigium*, che appunto significa traccia). Ma non siamo qui per occuparci di etimologia. Piuttosto ci interessa concentrarsi sul concetto di *"segno"*, *"orma"*, *"traccia"* appunto, e su dove possiamo trovarla. Il primo luogo di interesse è la scena del crimine, e questo oramai lo sanno anche le massaie dopo aver visto un'intera stagione di *"quarto grado"*; poi, in quest'epoca di sviluppo digitale, ci sono i device

tecnologici (smartphone, computer, tablet ecc.) che ci tracciano continuamente in ogni istante della nostra giornata. Ma c'è un altro luogo meno tangibile dove la traccia rimane impressa ed è così da sempre, prima della tecnologia e prima ancora che arrivassero Lombroso e i suoi seguaci: quel luogo è la mente di chi ha visto o sentito. In gergo giuridico il testimone o la persona informata dei fatti, a seconda della fase processuale in cui viene interrogata.
Se credete che recuperare quella traccia – detta traccia mnemonica – sia facile vi sbagliate, perché i meccanismi di memorizzazione, di elaborazione, le emozioni e le valutazioni di interesse giocano un ruolo fondamentale nella conservazione del ricordo e nella disponibilità a renderlo su richiesta. Certo, l'investigatore non può trasformarsi in uno psicologo, ma conoscere certi meccanismi gli consentirà di migliorare la capacità di procedere al colloquio investigativo e trarne la massima utilità. Detto questo, la testimonianza non solo è un mezzo per comprendere la dinamica dei fatti ma è soprattutto una prova molto considerata sia nel processo civile che in quello penale.

Il valore processuale della testimonianza

Facciamo solo un breve accenno all'inquadramento giuridico della testimonianza per comprendere come il ricordo di chi ha visto o sentito si possa spendere nel processo. La testimonianza è uno dei mezzi di prova che consiste nella dichiarazione resa da un soggetto su fatti dei quali abbia avuto conoscenza e che sono oggetto del giudizio in corso, ad esso ricollegabili, oppure che rilevano ai fini processuali. Vale nel processo civile ed in quello penale. Parliamone in estrema sintesi.

- **Nel processo civile** - È un mezzo di prova che le parti in causa possono esperire per dimostrare l'accadimento di un fatto che costituisce il fondamento di un diritto che si intende fare valere (art. 2697 c.c.). È prevista e disciplinata dagli artt. 2721 e seguenti del Codice Civile e dagli artt. 244 e seguenti del Codice di Procedura Civile. È importante ricordare che l'art. 246 cpc, rubricato *"incapacità a testimoniare"*, afferma che *"non possono essere assunte a testimoni le persone aventi nella causa un interesse che potrebbe legittimare la loro partecipazione al giudizio"*. Secondo la Suprema Corte (Cassazione Civile n. 11034/2006) si deve trattare di un interesse personale, concreto e attuale che possa comportare la legittimazione principale a proporre l'azione oppure una legittimazione secondaria ad intervenire nello stesso giudizio.
- **Nel processo penale** – Il contributo di chi era presente (oppure di chi ha appreso, nel caso della testimonianza de relato) è utilizzabile tanto in fase di indagine preliminare quanto – più significativamente - nel dibattimento. Nell'indagine preliminare si parla di *"persona informata dei fatti"* e il suo contributo è finalizzato alla comprensione della dinamica dell'evento da parte degli inquirenti. Nel dibattimento, fatta eccezione per il rispetto del principio *"nemo tenetur se detegere"* (cioè non essere mai costretti ad una autoaccusa) e salvi i casi d'incompatibilità previsti dalla legge, il testimone ha l'obbligo di rendere la testimonianza dicendo la verità e non nascondendo nessuna informazione. Il teste viene sottoposto all'esame delle parti e il giudice può fondare la propria decisione su quanto ascoltato.
- **Nell'indagine difensiva** - Tanto l'avvocato (specificamente incaricato) tanto i suoi ausiliari, quindi anche l'investigatore a sua volta incaricato, possono svolgere colloqui informali. Infatti, l'art. 191-bis cpp prevede che: *"per acquisire notizie il difensore, il sostituto, gli investigatori privati autorizzati o i consulenti tecnici possono conferire con le persone in grado di riferire circostanze utili ai fini dell'attività investigativa. In questo caso, l'acquisizione delle notizie avviene attraverso un colloquio non documentato"*. Poi, l'avvocato – quando ritiene utili le dichiarazioni informali alla propria strategia difensiva - può procedere all'intervista investigativa che, invece, è un atto formale.

Cerca il testimone

Se è importante comprendere il valore processuale della testimonianza, semplicemente perché fa prova, è ancora più importante saper individuare le persone informate dei fatti e saper trarre dalle stesse le informazioni più utili e significative. Raramente il testimone si fa avanti sua sponte. In questo senso il lavoro dell'investigatore è fondamentale, perché ricercare le persone informate e saperle ascoltare richiede abilità e metodo.

I testimoni e i loro ricordi

Comunemente si pensa che la memoria delle persone sia un processo semplice (come scattare una foto o registrare un video). È sba-

gliato: si tratta di un ambito caratterizzato da processi piuttosto complessi. Per rubare una riflessione al noto scrittore Primo Levi, possiamo dire che *"la memoria umana è uno strumento meraviglioso ma fallace. I ricordi che giacciono in noi non sono incisi sulla pietra: non solo tendono a cancellarsi con gli anni, ma spesso si modificano, o addirittura si accrescono incorporando elementi estranei. Lo sanno bene i magistrati* (ndr: quantomeno lo dovrebbero sapere): *non avviene quasi mai che due testimoni oculari dello stesso fatto lo descrivano allo stesso modo e con le stesse parole, anche se il fatto è recente e nessuno dei due ha interesse personale a deformarlo"*. Abbiamo detto tutto. Potremmo chiudere qui. Il fatto è che – come spiega lo scrittore – un ricordo troppo spesso evocato ed espresso in forma di racconto tende a fissarsi in uno stereotipo, in una forma collaudata dall'esperienza, cristallizzata, perfezionata, adornata, che si installa al posto del ricordo greggio e cresce a sue spese. Scordiamoci di pensare, allora, che la memoria sia solo un serbatoio dove i fatti percepiti vengono immagazzinati in modo statico.

I "magazzini della memoria"

L'evento percepito viene strutturato come esperienza cosciente: in altre parole una traccia mnestica che può essere successivamente rievocata. Ma esiste un solo *"magazzino"* dei ricordi? La risposta è no, perché ne esistono due: la memoria a breve termine (anche detta dagli psicologi "di lavoro") e quella a lungo termine. La memoria a breve termine immagazzina informazioni di rapida assimilazione e di sussistenza limitata, però è anche l'anticamera della memoria a lungo termine. Ma qual è il meccanismo che consente il passaggio dell'informazione da un sistema all'altro? È la reiterazione della traccia, la quale, una volta collocata nella memoria a lungo termine lì resta teoricamente (molto teoricamente) senza limiti di quantità e durata. Il problema, di cui l'investigatore deve tener conto, è che il passaggio non si fa con un click ma è un processo: sul percorso, reiterazione ed elaborazione cognitiva possono alterare la traccia. Se è consentita una similitudine è come trovare sulla scena del crimine una traccia di Dna (utile in quello stato), prelevarla e portarla in laboratorio. L'esperienza ci insegna che in tale processo la traccia può deteriorarsi o essere modificata. Può avvenire qualcosa di simile nel passaggio dell'informazione dalla memoria di lavoro a quella di lungo termine. Tornando perciò a quello che sapientemente diceva Primo Levi, il rischio è insito nel fatto che reiterazione ed elaborazione cognitiva del ricordo costituiscono non solo il modo di consolidarlo, ma anche occasioni per arricchire o modificarne i dettagli. Attenti quindi a quella che gli psicologi definiscono come "interferenza retroattiva", cioè alla contaminazione del ricordo; fenomeno da considerarsi senza meno nell'interrogare un teste.

Che cosa deve sapere l'investigatore?

Prima di giungere ad attuare un valido metodo per l'intervista, occorre conoscere i meccanismi attraverso i quali le persone codificano le proprie percezioni. La codifica rappresenta l'inizio: ciò che va dagli occhi (o dalle orecchie) al cervello e lì viene immagazzinato. La conoscenza del meccanismo di codifica offrirà all'investigatore un certo spazio di manovra quando si tratterà di chiedere la rievocazione del ricordo. La traccia mnestica si forma mediante un processo che si innesca nel momento percettivo (cioè quando si vede o si sente), prosegue con l'elaborazione interiore dei dati sensoriali e si conclude con la fissazione della memoria del fatto. In sintesi, le persone *"codificano"* interiormente ciò che percepiscono all'esterno non con un flash, ma attraverso dei passaggi.
È importante conoscere i fattori che condizionano la codifica per saper fare le giuste domande. I fattori che intervengono nella fase di codifica del ricordo sono tre: i *"fattori situazionali"*; le *"caratteristiche dello stimolo"*; *"le caratteristiche dell'osservatore"*.

- **I "fattori situazionali"** riguardano tutte le variabili legate al contesto ambientale, per definire le quali occorre porre alla persona informata dei fatti precise domande. Quanto è durata l'osservazione? Più è lungo questo tempo, più il ricordo potrà essere accurato. Quali erano le condizioni di luce? Non c'è dubbio che la penombra non aiuta la netta percezione e, di conseguenza, la codifica del ricordo. A che distanza Lei si trovava dalla scena? Di sicuro più è lunga la distanza meno è facile memorizzare i dettagli. Cosa stava facendo? Ovviamente se molto concentrato su altro (es. giocava alle slot machine) la percezione dell'evento sarà stata più fugace. Come si è mossa l'azione? Anche la velocità dell'e-

vento condiziona la codifica della percezione.

- **Le "caratteristiche dello stimolo"** riguardano, invece, il significato dello stimolo stesso: se il fatto è singolare o inusuale o foriero di particolari emozioni lo stimolo sarà più netto. Esagerando l'esempio, se l'investigatore chiede: mentre si trovava il 15 gennaio scorso lungo quella via affollata di gente, lei ricorda di aver visto passare un uomo con un cappotto grigio scuro? Ovvio che in questo caso lo stimolo è debole perché a gennaio per le strade della città non è così inusuale vedere persone con un cappotto scuro. Se invece avesse chiesto se quel giorno il teste avesse visto passare un signore in bermuda e canottiera e ciabatte, l'investigatore potrebbe confidare in un ricordo anche molto specifico riguardo ai dettagli. La differenza sta appunto nella caratteristica dello stimolo: perché gli stimoli più strutturati e dotati di significato si ricordano meglio.
- **Le "caratteristiche dell'osservatore"**: va da sé che la qualità del ricordo dipenda molto anche dalla capacità del soggetto di percepire gli stimoli e di comprenderli. Bisogna considerare che, di regola, l'apprendimento non è intenzionale ma incidentale. Così giocano un ruolo importante le reazioni emotive. Si pensi al soggetto che nell'assistere a un terribile sinistro automaticamente si copre gli occhi per non vedere più quelle paurose scene, oppure a chi assiste a un omicidio ed è colto dal terrore di poter restare a propria volta vittima. È stato provato che davanti ad episodi cruenti i soggetti possono addirittura andare incontro ad esperienze dissociative e quindi a fenomeni amnestici: in altri termini a un vuoto nella memoria.

Attenti alle distorsioni

Anche di fronte ad eventi non particolarmente cruenti si possono registrare delle distorsioni di codifica del ricordo. Distorsioni di ordine temporale ad esempio: gli eventi nella mente magari si susseguono più lentamente, o viceversa con una maggiore accelerazione, oppure in maniera cronologicamente disordinata. Poi si possono verificare distorsioni di carattere visivo: non sempre il teste ha uno sguardo panoramico d'insieme. C'è differenza tra guardare e vedere. Ci sono infatti casi in cui la sua vista si concentra su un dettaglio percepito come maggiormente significativo o pauroso. Gli esperti hanno studiato, per esempio, il fenomeno del cosiddetto *"weapon focus"* per il quale

È importante conoscere i fattori che condizionano la codifica per saper fare le giuste domande. I fattori che intervengono nella fase di codifica del ricordo sono tre: i "fattori situazionali"; le "caratteristiche dello stimolo"; le "caratteristiche dell'osservatore".

in presenza di armi esse tendono a catturare l'attenzione al punto che il teste non saprà riferire nient'altro. Peggio se a rendere la testimonianza è la vittima di una minaccia a mano armata: è stato riscontrato che in tali condizioni spesso la persona minacciata addirittura non è in grado di descrivere il volto del malvivente, nonostante ce lo avesse avuto di fronte per un discreto lasso di tempo a venti centimetri dal volto. Sempre nel novero delle distorsioni visive possiamo annoverare quelle relative alle differenze razziali. In una ricognizione fotografica attraverso cui individuare il responsabile tra i tanti volti effigiati, un conto è procedere con le foto di italiani o caucasici, altro conto è farlo con foto di cinesi. Quindi nessuna sorpresa se l'investigatore mostrando la foto al teste della persona di provenienza orientale si sentisse rispondere con la classica frase *"i cinesi sono tutti uguali"*. Quello che l'investigatore probabilmente ignora è che una risposta dello stesso tenore la otterrebbe viceversa mostrando a un teste cinese la foto di un italiano.
Infine, non devono essere trascurate le possibili distorsioni uditive: i suoni possono essere attenuati o amplificati nel ricordo.

L'acquisizione della traccia mnemonica

A sentire una persona, più o meno sono capaci tutti, ma ascoltarla è un'altra cosa: significa saperne trarre solo le informazioni che interessano traendole dalla sua memoria. Estrarre la traccia mnemonica richiede una abilità tecnica come - se è consentito fare un parallelo – per il tecnico estrarre la traccia di Dna o l'impronta digitale sulla scena del crimine. E non c'è bisogno di aggiungere altro per significare che il recupero della traccia mnestica è un momento piuttosto critico. Spesso non ci si fa caso, ma anche il contesto nel quale avvie-

Secondo la *"curva dell'oblio"*, elaborata da **Hermann Ebbinghaus**, psicologo e filosofo tedesco, precursore degli studi sperimentali sulla memoria, dopo solo 20 minuti abbiamo già perso il 40% dei dettagli di quanto abbiamo appreso, quota che scende al 30% trascorso solamente un giorno.

ne il colloquio è importante. In definitiva, più il contesto emotivo è simile a ciò che ha vissuto e più netta sarà la rievocazione. Sono quindi da evitare le formalità asettiche, oppure l'ascolto in luoghi inadatti (ad esempio in mezzo a un via vai per strada, o in un bar affollato, salvo che l'evento che si intende rievocare non sia avvenuto proprio in contesti del genere). In ogni caso nella fase del colloquio – cioè del recupero delle tracce mnestiche – giocano due fattori di rischio. Il primo è la cosiddetta *"interferenza retroattiva"*, cioè il condizionamento che inevitabilmente gioca sul ricordo, l'aver sentito parlare del fatto da altri, l'aver letto le interpretazioni dei media, l'aver ragionato sull'opportunità o meno di collaborare. Il secondo fattore di rischio è rappresentato dalla cosiddetta *"traumatizzazione secondaria"*, ma questo riguarda solo la memorizzazione di eventi traumatici e quindi l'ascolto delle vittime, oppure di chi è stato diversamente coinvolto in modo emotivamente molto forte. Infine, è importante anche considerare la *"freschezza"* della traccia, considerato che secondo la *"curva dell'oblio"*, elaborata dallo studioso **Hermann Ebbinghaus**, dopo solo 20 minuti abbiamo già perso il 40% dei dettagli di quanto abbiamo appreso, quota che scende al 30% trascorso solamente un giorno. Spetta quindi all'investigatore individuare in fretta le persone informate dei fatti e valutarne grossomodo il sincero intento collaborativo o meno.

Le regole da seguire

Su come si conduce un colloquio, una intervista investigativa o un interrogatorio, non esistono protocolli standard. Però gli studi condotti in proposito dagli psicologi della testimonianza possono offrire una valida linea da seguire.

1 | Chiarire chi siamo e la finalità dell'intervista - Sotterfugi, mascheramenti e trabocchetti non pagano perché prima o poi finiranno per compromettere la disponibilità a collaborare. Non bisogna dimenticare che il colloquio è una interlocuzione informale: se è finalizzato ad ottenere solo qualche informazione frammentaria o qualche indicazione molto specifica (tipo: lei conosceva l'uomo di cui hanno parlato i giornali? Frequentava questo Bar?) passi, ma se le cose oggetto del colloquio sono destinate ad essere cristallizzate successivamente in una deposizione, il gioco non paga. Quindi è bene prendere una posizione chiara rispetto alla quale l'interlocutore deciderà come comportarsi. Altra cosa che deve essere chiara è che l'intento dell'investigatore è quello di ricostruire un fatto nella sua verità storica, senza necessità di sviluppare considerazioni sulla responsabilità di chicchessia. L'atteggiamento di chiarezza e di asetticità servirà anche ad evitare l'insorgenza di fenomeni di compiacenza da un lato o, peggio, di falsificazione compiacente dei fatti dall'altro.

2 | Chiedere informazioni ma non fornirne - Attenzione, non dimentichiamo che anche la domanda è una forma di comunicazione. Essa stessa è una informazione che passa dall'investigatore al teste. Quindi, per evitare possibili distorsioni nelle tracce mnestiche nelle domande che si pongono bisogna cercare di non includere informazioni relative ai fatti che ci si attende essere narrati. Sarebbe come rilevare la traccia del Dna contaminandola con lo strumento utilizzato. Facciamo un esempio. Domanda: lei ha visto l'auto con cui è fuggito il killer? Questa domanda contiene diverse informazioni. La prima è che il malfattore è fuggito in auto; la seconda è che l'investigatore ritiene che il teste abbia visto l'auto; la terza è che quello che è fuggito è un killer, cioè un assassino di professione. Pensate davvero che quest'ultima informazione possa essere di stimolo alla testimonianza? Per minimizzare il rischio l'investigatore dovrebbe cercare di utilizzare nelle domande le informazioni che già ha appreso dal soggetto stesso. Non che sia una tecnica facile, perché richiede l'abilità di pervenire in modo graduale al completamento del racconto senza interferire. Meglio, dunque, chiedere di raccontare il fatto e poi, facendo domande più approfondite su ciò che è già stato riferito, giungere man mano a completare il quadro.

3 | Poni domande aperte - La persona deve avere la massima libertà di esprimersi; pertanto, gli vanno poste domande che presuppongono risposte altrettanto libere ed articolate. Tecnicamente si chiamano *"domande aperte"*. Al contrario devono essere evitate il più possibile le cosiddette domande chiuse, cioè quelle che presuppongono risposte brevi ed alternative di risposta ristrette (esempio: sì o no? È vero o falso? ecc.). Per inciso l'utilizzo di queste ultime sarà molto proficuo, invece, nell'esame dibattimentale da parte dell'avvocato. Ma nell'investigazione sarebbero controproducenti.

4 | Mai interrompere - Non è facile, perché nell'esperienza comune lo fanno tutti, spesso senza nemmeno accorgersene. Talvolta la comprensione di ciò che si ascolta è veloce e l'istinto dell'interlocutore è quello di chiedere, interrompendo il discorso, per ottenere risposte più specifiche. Nel colloquio investigativo, invece, è bene consentire alla persona di seguire il filo del suo pensiero senza interruzioni. Il momento degli approfondimenti, come già detto, inizia solo dopo che il soggetto ha completato la sua narrazione. Questo vale anche nel caso in cui il teste sia particolarmente prolisso o quando dimostri la tendenza a divagare. Si può tentare di riportarlo sul binario d'interesse, ma con molta cautela e delicatezza.

5 | Sostieni il silenzio e non riempire le pause - Se è necessario lasciare libera la narrazione, occorre per contro sostenere anche i silenzi. Il silenzio non deve essere interrotto. Un'altra pratica diffusa in modo inconsapevole è quella di riempire, di fronte a una pausa dell'interlocutore, le sue pause con le proprie parole. Invece, il soggetto deve avere modo e tempo per riordinare le idee così da poter arricchire ancora di più la propria dichiarazione. L'investigatore deve attendere senza distogliere da lui lo sguardo e al limite, se le pause si prolungano in modo spropositato, può incoraggiare il teste con cenni di assenso con la testa o limitate espressioni verbali, del tipo *"continui"*.

6 | Se si tratta della vittima, offrirgli il controllo del colloquio - Quando a riferire sui fatti è colui che li ha subiti, si profila un altro rischio: quello della cosiddetta *"vittimizzazione secondaria"*. Bisogna infatti considerare che rievocare un evento traumatico può riattivare le reazioni emotive vissute in precedenza e creare una condizione di difficoltà per la persona che viene ascoltata. Conviene quindi mettere in chiaro da subito che il colloquio si svolgerà nelle modalità e nei tempi più comodi per l'intervistato; che l'esame può essere interrotto a suo piacimento e ripreso successivamente. Chiarire queste cose fornisce alla persona ascoltata la sensazione di poter gestire e padroneggiare il colloquio e, in sostanza, di avere il controllo della rievocazione. Non si tratta di una sensazione banale: si ricordi che uno degli aspetti più traumatici vissuti mentre si subisce un evento dannoso è la percezione di non poter controllare ciò che sta accadendo. Un terribile senso di impotenza. Controllare la rievocazione, quindi, evita di rivivere la stessa sensazione di vulnerabilità.

7 | Non caricare di una responsabilità chi parla - Di fronte al soggetto, il peso di ciò che sta dicendo va calibrato. Se il soggetto percepisce che attribuiamo il massimo valore a ciò che sta dicendo nella determinazione delle responsabilità altrui, potrebbe essere colto da ansia e disagio, se non talvolta da un qualche timore. Questo inciderà inevitabilmente sulla sua spontaneità. Viceversa, non si deve nemmeno infondere nel soggetto il senso dell'inutilità di ciò che sta dicendo, perché questo potrebbe condizionare l'accuratezza del racconto.

In definitiva, la codificazione di un ricordo è contrassegnata da diversi passaggi e la rievocazione, durante il colloquio o l'intervista investigativa, presuppone altrettanti passaggi. Come volevasi dimostrare sentire è una cosa che sanno fare tutti, ascoltarla è ben altra cosa: è una cosa da investigatore, appunto.

Chi è Ugo Terracciano

Nato a Padova nel 1960, **Ugo Terracciano** è laureato in giurisprudenza presso l'Università di Bologna e abilitato alla professione di avvocato presso la Corte d'Appello dello stesso capoluogo. Già docente di Tecniche Investigative presso l'Università di Bologna e oggi titolare degli insegnamenti di criminologia e di diritti umani e sicurezza presso l'Università **Unimercatorum**, Terracciano ha ricoperto diversi incarichi nella Polizia di Stato come dirigente e tiene docenze in ambito professionale, in quello dell'alta formazione e in master universitari a Bologna, Siena e L'Aquila. È docente di materie giuridico professionali presso la Scuola Ispettori della Guardia di Finanza de L'Aquila. Ha tenuto numerose relazioni in convegni nazionali e internazionali in materia di sicurezza, immigrazione, danno da sinistro stradale e indagini penali. Oltre che autore di pubblicazioni su riviste specializzate, è autore di diversi libri.

Giustizia predittiva: il dibattito è aperto

Luci e ombre sull'uso degli algoritmi di Intelligenza Artificiale nella giustizia civile, una nuova sfida per gli operatori di giustizia e per gli investigatori.

di Francesco Sardi de Letto

La giustizia civile attuale deve confrontarsi con un'attualissima constatazione: spesso non riesce a rispondere alle esigenze dei cittadini del XXI secolo. Difatti, i tempi della giustizia sono eccessivamente lunghi, i costi alti e la qualità - ahimè - non sempre elevata.
Nell'era digitale, anche il diritto viene (e verrà) sempre più influenzato dall'Intelligenza Artificiale, usata, come nella famosa profezia di Isaac Asimov, per rispondere alle domande umane e per dirimere i conflitti. Ad oggi, non c'è una definizione unitaria di Intelligenza Artificiale, taluni l'hanno definita come quel meccanismo basato sull'apprendimento che gli umani usano per prendere le decisioni quotidiane. Cioè la capacità di un sistema tecnologico - hardware e software - di fornire prestazioni assimilabili a quelle dell'intelligenza umana, risolvendo problemi o svolgendo compiti e attività tipiche della mente e del comportamento umano. Ciò presuppone la

capacità non soltanto di trattare automaticamente enormi quantità di dati e fornire le risposte per le quali tali sistemi sono stati programmati, ma anche di acquisire, sulla base di appositi algoritmi di apprendimento, l'attitudine a formulare previsioni o assumere decisioni.

Una sfida per l'operatore di giustizia

Di fronte a ciò, l'operatore di giustizia, naturalmente, annoverando anche l'investigatore privato, si trova così a doversi confrontare con una nuova sfida, quella della "giustizia predittiva". Concetto che dovrà, giocoforza, essere al centro del nostro pensiero, dei nostri progetti e della nostra attenzione.
Credo che tutti noi non possiamo e non dobbiamo abdicare al nostro ruolo professionale, ma per essere in grado di governare il fenomeno incipiente dell'AI dobbiamo imparare a conoscerlo, rifuggendo sia da toni eccessivamente entusiastici, consegnandoci e demandandoci fideisticamente a una integrale decisione robotica, sia da quelli scettici e pessimistici, volti a escludere totalmente l'uso degli strumenti offerti dall'AI, perché vorrebbe dire privarci in radice di un possibile miglioramento del sistema giustizia. Occorre invece, facendo appello a tutto il nostro equilibrio, competenza e capacità di approfondimento, utilizzare le potenzialità offerte dalla tecnologia e dagli algoritmi di Intelligenza Artificiale, come se fossero dei moltiplicatori di qualità, sapendo di avere a fianco un supporto volto a favorire una riduzione di tempistica nell'elaborazione dei nostri incarichi professionali.

In cosa consiste la giustizia predittiva

La giustizia predittiva consiste, stricto sensu, nella capacità informatica di rendere usufruibile rapidamente un certo flusso di informazioni per anticipare la probabilità delle decisioni. Detto ciò, risulta molto variegato il panorama di definizioni correlato al termine *"giustizia predittiva"*; l'espressione più generalizzata specifica il fenomeno come il ricorso a tutte le innovazioni digitali nel campo del diritto e, allo stesso tempo, come lo strumento informatico, fondato su una base di dati giurisprudenziali, che con l'aiuto di specifici algoritmi, permette di anticipare quali saranno le probabilità statistiche di successo in una vicenda giudiziale.
La giustizia predittiva non ci fornisce quindi la profetica sfera di cristallo, ma ci può aiutare a determinare, per mezzo dell'applicazione di tecniche quantitative (cioè gli algoritmi di Intelligenza Artificiale), le probabilità di ogni possibile esito di una controversia o di un'indagine. Pertanto, alla luce di quanto sopra detto, la giustizia predittiva apre uno spiraglio giuridico per gli operatori del diritto e per la stessa scienza del diritto.
Non possiamo certo nascondere che ciò, all'evidenza, porti con sé il rischio di un dominio del virtuale sul reale, quando la giustizia predittiva, in una non auspicabile sua degenerazione, possa rappresentare in via assoluta un elemento prescrittivo per i professionisti, ovvero dissuasivo per i richiedenti giustizia.
Difatti, le nuove tecnologie, in primis l'Intelligenza Artificiale con il relativo trattamento dei dati, contribuiranno a modificare non soltanto il ruolo dei giuristi e degli agenti economici ma anche il modo in cui essi applicheranno il diritto alla luce della raccolta e della catalogazione su larga scala delle decisioni giudiziarie e della messa a disposizione dei dati con il trattamento automatizzato degli stessi. In quest'ottica, l'AI permetterà di rendere intellegibili una quantità impressionante di dati e, attraverso delle valutazioni di probabilità effettuate mediante correlazioni, permetterà di essere edotti, ad esempio, circa le probabilità di rigetto di una determinata istanza giudiziale in uno specifico settore. Il terrore che la profezia di Asimov si concretizzi ci porta a considerare l'ipotesi se sul medio-lungo termine vi possa essere un concreto rischio di vedere operativi degli avvocati robot.
L'auspicio è che la giustizia predittiva non possa provocare la scomparsa degli avvocati e degli operatori del diritto, ma piuttosto finirà con l'automatizzare solo un certo tipo di lavoro *"para legale"*, quale per esempio la predisposizione e gestione di dossier ripetitivi e semplici (vie-

Per utilizzare le potenzialità offerte dalla tecnologia e dagli algoritmi di Intelligenza Artificiale, occorrono competenza e capacità di approfondimento. Questi strumenti vanno utilizzati come moltiplicatori di qualità e come un supporto volto a favorire una riduzione di tempistica nell'elaborazione dei nostri incarichi professionali.

ne alla mente la redazione di atti massivi quali ricorsi per ottenere provvedimenti monitori su larga scala, atti di precetto, esecuzioni ingenti a favore di società che hanno acquistato numerosi crediti da esigere). Correrà il rischio di essere sconvolta la relazione tra clienti e professionisti del diritto: il cliente potrà in anticipo venire a conoscenza circa la previsione dell'esito della controversia (magari, senza fidarsi totalmente della parola del professionista), avendo anche una base per una determinazione preventiva molto precisa dei costi.
Se da un lato l'utilizzo della giustizia predittiva porterà vantaggi in termini di tempo e produttività, per contro, il suo utilizzo non ragionevole potrà condurre inevitabilmente a dei rischi. Innanzitutto, quello dell'automatizzazione e standardizzazione delle decisioni giuridiche con lo sgradito effetto di un concreto rischio di conservatorismo e rigidità delle decisioni, poiché le previsioni proverrebbero da ciò che è già stato giudicato e la giurisprudenza cesserebbe così di evolvere (l'evoluzione giurisprudenziale è un elemento fondamentale nell'evoluzione della società). A tal riguardo, non si vuole credere che i magistrati non osino più prendere decisioni divergenti e che il potere legislativo non intervenga in subjecta materia, permettendo invece la denegata evoluzione di un algoritmo performativo, con una sorta di profezia auto-realizzatrice, che finirebbe per distorcere il mondo reale per farlo corrispondere alla propria anticipazione predittiva.
Inoltre, si prospetterebbe un rischio di parzialità (la tomba del diritto), se gli algoritmi fossero mal concepiti rendendo la predizione giuridica non più *"neutra"* (si veda, quanto accaduto nel così detto programma *"Compas"*, utilizzato per stimare il rischio di recidiva di condannati negli Usa dell'anno 2016, che è stato accertato possedere un basso tasso di affidabilità, poiché sfavoriva la popolazione afroamericana).

Il controllo della tecnologia

Tuttavia, il vero tema centrale sarà il seguente: in tale prospettiva chi avrà realmente il controllo di questa tecnologia? In altre parole, potrà esserci un evidente pericolo di dipendere da grandi gruppi, che non saranno più sotto il controllo pubblico e potranno imporre la loro visione economica e giuridica della società, permettendo un utilizzo scorretto delle nuove tecnologie per colpire le libertà individuali e i valori democratici.
Il rischio maggiore all'interno di questa prospettiva è quello che discende dal collegamento tra Intelligenza Artificiale e possibile destabilizzazione del diritto: il rischio di una giustizia artificiale che intacchi l'indipendenza e l'imparzialità del giudice, che sono in assoluto pietre angolari di una buona giustizia.
Il giudice potrebbe rischiare di essere influenzato dagli strumenti di giustizia predittiva, sapendo che la sua giurisprudenza verrà osservata, quantificata, misurata e, di conseguenza, sarebbe indotto a modificarla, venendo meno a un cardine dell'attuale sistema democratico, a suo tempo teorizzato da Montesquieu: l'indipendenza della magistratura, quale requisito per la sua imparzialità.
Quindi, lo sviluppo perverso degli strumenti di giustizia predittiva potrebbe causare un indebolimento dell'autorità della giustizia, profilando – altresì – la possibilità di un diritto superficiale, statico e rivolto al passato, con un irreversibile impoverimento della ricerca giuridica. Va da sé, che l'unico strumento di controllo dovrà consistere in una legge che perimetri e definisca gli obblighi deontologici dei magistrati nell'utilizzo degli strumenti di giustizia predittiva, secondo un'etica dell'Intelligenza Artificiale applicata al diritto. Non va, tuttavia, negato che l'AI può costituire anche una fonte unificatrice per il mondo del diritto, dacché potrà crearsi un meritorio movimento che possa mettere fine alla divisione tra sistemi giuridici di *Civil Law* e di *Common Law*, per farli convergere verso una nuova dimensione che qualcuno ha battezzato *"diritto isometrico"* (il cosiddetto *"Isometric Law"*), vale a dire un sistema giuridico nel quale l'integralità delle decisioni di giustizia sarà misurata in modo uguale da un programma informatico, la cui sintesi finisce per divenire essa stessa norma. Sarà vera gloria? Personalmente, penso di no. Difatti, si potrebbe argomen-

tare a riguardo che l'ufficio del giudice rischierebbe di essere modificato nella misura in cui il suo ragionamento potrebbe doversi adattare al diritto isometrico. Nei paesi di diritto civile, il giudice applica la legge ai casi particolari, e ciò è garanzia del rispetto della separazione dei poteri e dell'uguaglianza tra i cittadini sottoposti a una stessa regola. Con la giustizia predittiva, il giudice dovrebbe verificare se il caso da giudicare è identico o simile, secondo il software che implementa gli algoritmi di giustizia predittiva a uno o più processi già giudicati. Infine, con la giustizia predittiva, tutte le informazioni contenute nelle decisioni – tanto i giudizi di merito quanto le sentenze della Cassazione – faranno autorità, salvo che il programma non gerarchizzi le decisioni.

Luci ed ombre dell'AI

Attraverso l'uso degli algoritmi e, quindi, dell'Intelligenza Artificiale, non si dovrà in alcun modo sostituire l'attività del professionista. Per quanto concerne gli operatori del diritto, il ricorso agli algoritmi consente più facilmente di conoscere, seppur in termini prognostici e statistico-probabilistici, l'esito del giudizio e, quindi, di poter evitare liti che si possano rivelare temerarie e ricorrere a vie alternative di soluzione delle controversie quali: mediazione, negoziazione assistita, arbitrato laddove fossero più convenienti per le parti, con conseguente deflazione del contenzioso e risparmio di costi processuali inutili, prodotti anche dal fatto che, se le parti giungono a una soluzione condivisa, vi sarà un meno frequente utilizzo delle impugnazioni (con conseguente aggravio del contenzioso). Cionondimeno, il limite fondamentale all'uso della giustizia predittiva dovrà essere costituito dal rispetto dei principi fondamentali del giusto processo. Tali principi sono consacrati nella Convenzione europea dei diritti dell'uomo e dalle norme costituzionali, in particolare dagli artt. 25 (diritto al giudice naturale precostituito per legge) e 111 (giusto processo) Cost.
In linea puramente teorica, il diritto di adire il giudice non sarebbe compromesso se la giustizia predittiva conferisse al ricorrente scarsissime chances di successo a fronte di un'elaborazione eseguita da un software, quindi la mancata previsione di ipotesi di successo non costituisce un ostacolo alla ricevibilità dell'istanza.
Tuttavia, potrebbe accadere che, a fronte di un uso smodato e improprio del software di giustizia, il legislatore potrebbe prevedere in ordine a basse possibilità di successo o, addirittura, a una possibilità (predittiva) di fallimento dell'iniziativa pari al 100%, la non opportunità di coltivare l'iniziativa giuridica. Ciò sarebbe anche costituzionalmente improponibile.
La situazione sarebbe ben diversa, nel caso in cui a esito della consultazione del software di giustizia predittiva si prospettassero delle previsioni di successo molto alte per una parte e molto basse per l'altra. In tal caso, infatti, la parte che vanta un'alta possibilità di successo potrà imporre alla controparte di negoziare su questa base. Di conseguenza, la giustizia predittiva condurrà allo sviluppo di metodi alternativi di soluzione delle controversie a beneficio del sistema giustizia alleviandone anche i relativi costi.
Ma la giustizia predittiva comporterà anche il rischio (non trascurabile) di un forte incentivo alla rinuncia ad adire le vie giudiziali. Questa rinuncia è lecita se è realizzata con conoscenza di causa e in modo non equivoco (un risultato affidabile deve nascere da statistiche non contestabili) ma, soprattutto, senza costrizioni. Il diritto di agire in giudizio va contemperato con l'esigenza di prevenire casi di abuso del processo, come ad esempio il contenzioso temerario, ma non potrà mai contemplare il divieto a rivolgersi alla Giustizia.

L'auspicio è che la giustizia predittiva non provochi la scomparsa degli avvocati e degli operatori del diritto, ma venga utilizzata per automatizzare solo un certo tipo di lavoro "para legale", quale per esempio la predisposizione e gestione di dossier ripetitivi e semplici.

Gli algoritmi e l'autonomia del giudice

In tale logica, sussiste un notevole problema riguardo alla qualità, all'affida-

bilità, alla correttezza e alla trasparenza dell'informazione, nonché alla necessità di integrare la giurisprudenza con la dottrina. Per esempio, un algoritmo che prendesse in considerazione solo la giurisprudenza passata, senza considerare il fatto che una nuova legge o un revirement della giurisprudenza abbia mutato il regime giuridico applicabile, darebbe dei risultati errati e ingannevoli. Ne deriva la considerazione secondo cui la giustizia predittiva non può sostituirsi in alcun modo all'atto del giudicare, che consiste nel rendere una sentenza motivata in fatto e in diritto solo sulla base di elementi dibattuti in contraddittorio.
In questo ambito, gli strumenti di giustizia predittiva, se utilizzati durante il processo, obbediranno ai principi delle regole processuali (procedura) e saranno sottoposti come gli altri elementi alla dialettica in contraddittorio. Se utilizzati in tal modo, gli strumenti di giustizia predittiva potrebbero arricchire i dibattiti giudiziari, contribuendo a definire e precisare l'equilibrio tra prevedibilità e imprevedibilità, necessario nell'esercizio della giustizia. Inoltre, l'utilizzo nel settore giustizia degli algoritmi consentirebbe al giudice di trovare più velocemente soluzioni a tema dibattuto in una controversia, dato che avrà la possibilità di analizzare in breve tempo una quantità di dati immessi nel sistema informatico molto più ampia (i cosiddetti big data) rispetto a quanto è solitamente in grado di fare un essere umano. Una soluzione sostenibile potrebbe essere rappresentata da un algoritmo che selezioni in modo intelligente l'informazione in una banca dati, anticipando delle informazioni all'utilizzatore, senza imporre alcuna soluzione, riservando al medesimo la responsabilità di usare in modo pertinente i risultati, anche in rapporto al caso di specie. Naturalmente, l'uso degli algoritmi di Intelligenza Artificiale risulta più agevole nelle cause ripetitive, semplici e di modesta entità. Più spinoso è l'utilizzo della giustizia predittiva nell'individuazione di parametri di credibilità di un testimone: a tal riguardo, soccorre la cosiddetta psicologia della testimonianza che, in alcuni casi, può essere codificata.
Resta, comunque, fermo che al giudice deve essere riservato un ruolo autonomo per valutare le prove e per decidere in che misura discostarsi dal responso dell'algoritmo, non potendo mai configurare una comoda modalità per giungere alla decisione anticipata.
Gli algoritmi sono strumenti di semplificazione e razionalizzazione del sistema, promuovono la calcolabilità giuridica, in quanto è possibile pervenire ad una interpretazione della legge prevedibile, e dunque rendere conoscibile *ex ante* l'esito dell'interpretazione della legge sul piano pratico. Un particolare ambito nel quale ciò potrà senza dubbio avvenire è quello degli indennizzi in materia di licenziamenti, in materia di ingiunzioni per pagamento di somme, nelle controversie di sfratto: tali casi verrebbero risolti dall'applicazione mediata di un algoritmo e al giudice non resterebbe che controllare che i dati iniziali immessi nell'algoritmo siano completi, mirati, affidabili e che le varie fasi del procedimento si siano correttamente compiute.

Il principio di uguaglianza delle parti

In chiave problematica va vieppiù considerato il rispetto del principio dell'uguaglianza delle parti, indispensabile per garantire un giusto processo. Quindi, potrebbero porsi dei problemi in relazione al fatto che l'utilizzo della giustizia predittiva richieda il ricorso a imprese fornitrici che hanno elaborato software specifici e li sfruttano commercialmente. Questa attività si sviluppa in un contesto di liberalizzazione di piattaforme *(legal tech),* elaborate da imprenditori associati a informatici che sviluppano tali prodotti, non essendo giuristi e in assenza di una sorveglianza della pubblica amministrazione. Le conseguenze sono importanti, infatti solo chi ha i mezzi per potersi permettere i servizi di queste imprese ne trae vantaggio.
Gli utilizzatori più solidi finanziariamente – banche, grandi imprese, compagnie di assicurazione ecc. – potranno così scegliere i risultati che sono loro favorevoli (quando non ne siano loro stessi i produttori), utilizzando i vari software di giustizia predittiva e negoziare con la controparte sulla base di tali risultati che talvolta, pro-

prio in ragione dello squilibrio di forze tra le parti, risultano essere falsati, poiché ne risulterà una situazione privilegiata per il richiedente che si trova in una posizione di vantaggio economico. Si potrebbe obiettare che già oggi tale ineguaglianza è presente nel nostro sistema in caso di controversia tra una parte forte (datore di lavoro o impresa) che può ricorrere a consulenze o assistenze professionali di grande qualità, di fronte a una parte debole (consumatore o lavoratore), che non può far fronte a spese equivalenti. Certo è che residua una sostanziale differenza: i risultati forniti dall'algoritmo di giustizia predittiva apparirebbero come evidenti e incontestabili, i pareri dei consulenti resteranno sempre passibili di smentita rispetto ad altri pareri diversamente formulati da colleghi.

Nemmeno la presenza di un software unico, pubblico e gratuito, potrebbe risolvere il problema, anzi da un certo punto di vista lo aggraverebbe. Infatti, un software unico presuppone che si possano con certezza valutare i risultati futuri dei processi alla luce di un solo metodo. Ciò oltre ad essere discutibile dal punto di vista tecnico potrebbe far scaturire l'evenienza che una sola previsione centralizzata tenderebbe ad assumere i connotati di verità unica e, come tale, finirebbe per influenzare il giudice e il suo relativo potere. Sarebbe una soluzione manichea, che vedrebbe relegati all'interno di due mondi distinti i giuristi fautori dell'accettazione incondizionata degli algoritmi all'interno di ogni procedimento civile e coloro che, ponendosi in una visione scettica, propendono verso il loro deciso rifiuto.

Al giudice deve essere riservato un ruolo autonomo per valutare le prove e per decidere in che misura discostarsi dal responso dell'algoritmo, non potendo mai configurare una comoda modalità per giungere alla decisione anticipata.

Alcuni bastioni invalicabili

In conclusione, i principi fondamentali del processo devono essere considerati dei bastioni invalicabili contro taluni pericoli della giustizia predittiva e l'AI dovrà rappresentare un'opportunità per tutti gli operatori del diritto, quindi integrativa e mai sostitutiva. Va doverosamente ricordato ciò che era solito dire Immanuel Kant: *"sapere aude"* (osa sapere). Ciò va esteso all'uso dell'Intelligenza Artificiale e all'ammonimento di essere sempre vigili nel pilotare con efficacia la trasformazione della giustizia, dando delle regole all'applicazione degli algoritmi in un settore così delicato. Ricordiamoci che la nostra mente sarà sempre indispensabile solo se sapremo essere profondi e attenti, non mai superficiali. In altre parole, dobbiamo cercare di essere insostituibili nel nostro lavoro e ciò avverrà se sapremo essere dei fuoriclasse. Nessuna intelligenza artificiale potrà mai prevalere sui fuoriclasse.

Chi è Francesco Sardi de Letto

Avvocato e professore, **Francesco Sardi de Letto** è nato a Vicenza nel 1961. Si è laureato in giurisprudenza presso l'Università degli Studi di Pavia nel 1984 ed è abilitato all'esercizio della professione forense dal 1989 e al patrocinio avanti le Giurisdizioni Superiori dal 2001. Titolare dello **Studio Legale Sardi de Letto**, in Brescia, si occupa di competenze legali tanto in ambito di consulenza stragiudiziale (anche per il tramite di consultazione on-line e in videoconferenza), quanto in ambito giudiziale. Lo Studio si occupa in prevalenza di diritto civile, in particolare contrattualistica, diritto del lavoro, diritto fallimentare e diritto sportivo. Nel 2019, **Universitas Mercatorum** di Roma ha conferito all'avvocato Sardi de Letto la cattedra di professore a contratto del corso di contrattualistica. Negli ultimi tempi, in forza della collaborazione con **Federpol**, lo Studio ha sviluppato approfondimenti sull'utilizzo delle prove investigative nell'ambito del processo civile.

Le nuove frontiere tecnologiche della delinquenza

Marcello La Bella, dirigente del Centro Operativo Sicurezza Cibernetica "Sicilia Orientale", racconta l'azione di prevenzione e contrasto della criminalità informatica, svolta a garanzia dei valori costituzionali della segretezza e della libertà di ogni forma di comunicazione.

di Laura Reggiani

La rapida diffusione dell'uso di Internet quale mezzo di scambio di informazioni, di accesso alle grandi banche dati, di esecuzione di transazioni e disposizioni finanziarie, di ideazione e creazione di nuove attività professionali, ha ben presto messo in evidenza i punti di debolezza della Rete, in particolar modo con riferimento alla sicurezza informatica. È in questo scenario che nasce la **Polizia Postale e delle Comunicazioni**, quale "specialità" della **Polizia di Stato**. Si tratta di un organismo all'avanguardia nell'azione di prevenzione e contrasto della criminalità informatica e a garanzia dei valori costituzionali della segretezza della corrispondenza e della libertà di ogni forma di comunicazione. La Polizia Postale e delle Comunicazioni è presente su tutto il territorio nazionale attraverso i 20 compartimenti, con competenza regionale e le sezioni con competenza provinciale, coordinati a livello centrale. Come ci ha raccontato il dottor **Marcello La Bella**, dirigente del **Centro Operativo Sicurezza Cibernetica** della **Polizia Postale** della Sicilia Orientale, che abbiamo avuto modo di conoscere e ascoltare in occasione del 66° Congresso Nazionale di **Federpol** che si è tenuto a Giardini Naxos lo scorso maggio, il principale sforzo operativo della Polizia Postale e delle Comunicazioni va oggi nella direzione del continuo adeguamento della propria risposta alle nuove frontiere tecnologiche della delinquenza.

Lo scorso anno è stata istituita la Direzione centrale per la sicurezza cibernetica in cui sono confluiti i reparti della Polizia Postale. Come è organizzata oggi la vostra struttura, quali sono le vostre competenze e quali gli obiettivi? Quali sono i rapporti con le altre forze a livello internazionale?

Nell'ambito del Dipartimento di Pubblica Sicurezza la legge ha istituito la Direzione centrale per la Polizia scientifica e la Sicurezza cibernetica, nel cui ambito opera il **Cert** *(Computer Emergency Response Team)* del Ministro dell'Interno, struttura incaricata di supportare le articolazioni ministeriali in caso di incidenti o attacchi informatici contro infrastrutture e reti dell'Amministrazione. Dalla Direzione dipendono i **Cosc** *(Centri Operativi di Sicurezza Cibernetica)* uffici di livello regionale della Polizia di Stato che hanno sostituito i vecchi Compartimenti Polizia Postale e delle Comunicazioni regionali, e alle cui dipendenze sono poste le Sezioni di Sicurezza Cibernetica provinciali già Sezioni Polizia Postale e delle Comunicazioni. I nuovi reparti, con una struttura organizzativa più aderente alle nuove esigenze, hanno assorbito le competenze della Polizia Postale, che in generale svolge una azione di prevenzione e contrasto della criminalità informatica e a garanzia dei valori costituzionali della segretezza e della libertà di ogni forma di comunicazione, operando in settori quali: protezione delle Infrastrutture Critiche del Paese, pedopornografia, cyberterrorismo, tutela del diritto d'autore, reati contro la persona commessi online, hacking, frodi informatiche, e-banking, giochi e scommesse online. Di fondamentale importanza nel contrasto del cybercrime sono le collaborazioni internazionali con gli omologhi Uffici di Polizia stranieri. Il Servizio centrale della Polizia Postale e delle Comunicazioni costituisce il punto di contatto dell'Italia con gli uffici di polizia dei Paesi aderenti al G8 che si occupano di crimini informatici. Inoltre, per rendere più incisiva la strategia di contrasto al crimine informatico, la Polizia Postale, oltre ai canali di interscambio di informazioni, partecipa, con alcuni suoi rappresentanti, a gruppi di lavoro permanenti, istituiti dal Governo o da organismi internazionali, tra cui il Gruppo Interministeriale per la sicurezza delle reti, il G8, la Comunità Europea, il Consiglio d'Europa, l'Ocse, l'Interpol e l'Europol.

Quali sono le doti personali e le competenze professionali che deve possedere chi opera nel vostro ambito d'indagine?

Ovviamente, deve possedere le doti che vengono richieste a tutti i poliziotti: ad esempio, senso di responsabilità e del dovere, equilibrio, controllo emotivo. Per l'impiego nell'ambito della Polizia Postale occorre avere attitudini investigative ed essere già in possesso di un buon bagaglio di conoscenze nel campo informatico e dei servizi della Rete. Le conoscenze tecniche saranno ulteriormente sviluppate grazie ai corsi specialistici che saranno frequentati, quasi tutti di alto livello tecnico-professionale.

Di che tipologia di collaboratori vi avvalete e quali strumenti utilizzate? Quali sono i professionisti che vi affiancano nelle indagini? Esiste, o potrebbe esistere, una collaborazione con gli investigatori privati?

Nelle nostre attività investigative potrebbe presentarsi la necessità di fare ricorso a competenze esterne molto specialistiche. Ad esempio, nell'ambito del cyberterrorismo può essere necessaria la figura di un interprete durante il monitoraggio della rete, così come in materia di pornografia minorile alcune volte ci si è avvalsi di esperti ai fini della identificazione delle minori vittime o degli abusanti. Potrebbe, ovviamente, anche essere utile un investigatore privato nel momento in cui dovesse fornire elementi importanti in una indagine ottenuti nell'ambito del suo incarico di parte o, anche, avuti in via incidentale.

Il lavoro della polizia postale è stato quanto mai prezioso negli anni della pandemia. Come è cambiata la criminalità in questi ultimi anni e quali sono i reati digitali maggiormente commessi online?

La pandemia ha visto un notevole aumento di tutti i reati commessi online, complice la necessità, soprattutto nei periodi di restrizioni, di trascorrere più tempo connessi ma, forse, anche la situazione di generale incertezza diffusa nella popolazione. In particolare, delitti relativi allo sfruttamento sessuale di minori, frodi online ed attacchi a sistemi informatici sono raddoppianti rispetto ai periodi pre-covid. E si sono diffuse azioni che, tramite la sostituzione di persona, realizzano attacchi **Bec** *(Business Email Compromise)*, phishing e ransomware.

Il cybercrime è una emergenza mondiale e in periodo pandemico stati portati avanti molteplici attacchi verso le infrastrutture critiche, come gli ospedali, ma anche verso le aziende private. Come si sono evoluti e come potranno evolversi in futuro i cyberattacchi?

Come di recente è stato evidenziato da un report del **Censis** che si rifà ai dati della Polizia postale, nel 2022 gli attacchi informatici alle infrastrutture critiche sono più che raddoppiati rispetto all'anno precedente incrementandosi di quasi il 140%, e tra il 2012 e il 2021 i reati informatici denunciati all'autorità giudiziaria dalle forze di polizia sono più che raddoppiati, registrando una crescita superiore al 150% in controtendenza con l'andamento decrescente del totale dei reati che, nello stesso periodo di tempo, si sono ridotti di oltre il 25% .Vi è da aggiungere che la moltiplicazione delle azioni criminali contro le istituzioni, le aziende e i privati potrebbe essere, anche, un riflesso di quello che è l'attuale scenario di guerra, dove all'azione del

Di cosa si occupa la Polizia Postale e delle Comunicazioni

A livello operativo il Servizio è organizzato in distinte aree d'intervento.

- **Pedopornografia** - Attraverso il Centro Nazionale per il contrasto della pedopornografia su Internet la Polizia Postale e delle comunicazioni raccoglie segnalazioni, coordina le indagini sulla diffusione, in Internet o tramite altre reti di comunicazione, delle immagini di violenza sessuale sui minori e stila le black list dei siti web pedofili.
- **Cyberterrorismo** - Una qualificata squadra di investigatori monitora costantemente la rete Internet e conduce indagini specialistiche sul sempre più diffuso utilizzo delle nuove tecnologie di comunicazione da parte dei gruppi antagonisti ed eversivi nazionali e stranieri.
- **Copyright** - I circuiti di condivisione di file (file sharing) e i numerosi altri servizi Internet che consentono la circolazione di opere dell'ingegno hanno contribuito alla diffusione illegale di file e hanno imposto un'attenzione operativa costante al fenomeno.
- **Hacking** - Tutti coloro che utilizzano la Rete Internet per danneggiare o per colpire, tramite la stessa, obiettivi a essa correlati sono oggetto di attenzione da parte degli investigatori.
- **Protezione delle infrastrutture critiche del Paese** - Le aziende e gli enti che sostengono e garantiscono il funzionamento del Paese mediante reti e servizi informatici o telematici vengono monitorati e protetti da attacchi informatici attraverso l'azione di un'equipe di investigatoti specializzati nel contrasto del cybercrime, appartenenti al *Centro Nazionale Anticrimine Informatico per la protezione delle Infrastrutture Critiche.*
- **E-banking** - Le nuove frontiere del commercio e della circolazione di denaro impongono un puntuale monitoraggio delle risorse tecnologiche correlate con la finalità di garantirne la sicurezza.
- **Analisi criminologica dei fenomeni emergenti** - Una qualificata equipe di psicologi e investigatori analizza ed elabora dati relativi alle nuove frontiere del crimine informatico, ponendo il sapere clinico e criminologico delle scienze sociali al servizio di una più efficace azione di prevenzione e repressione dei reati informatici.
- **Giochi e scommesse online** - Attraverso il monitoraggio della Rete e un'attenta analisi dei siti dedicati si individuano le attività non autorizzate dal Ministero delle Finanze - Amministrazione autonoma monopoli di Stato.

cyber crime ordinario si aggiungono gli attacchi con strumenti cyber offensivi da parte di hacker criminali che fanno della guerra cibernetica una componente del più ampio conflitto. L'attenzione da parte del Servizio di Polizia Postale e dei dipendenti Centri Operativi di Sicurezza Cibernetica è quanto mai alta proprio per assicurare un'adeguata protezione a istituzioni imprese e cittadini. In questo contesto è innegabile che i cyber criminali affineranno sempre più i loro strumenti di attacco dirigendo verosimilmente le loro azioni criminali anche verso l'Internet of Things e l'Intelligenza Artificiale.

Anche il gaming e le scommesse abusive online rappresentano un problema con cui vi confrontate?

Il contrasto del gioco d'azzardo illegale online è tra le nostre attività istituzionali. Sul punto, basti ricordare una delle operazioni di polizia giudiziaria tra le più importanti denominata *"Master Bet"*. L'indagine si è conclusa con l'arresto di 13 persone e la denuncia di altre 107 nonché con il sequestro di 46 centri scommesse ubicati in numerose città italiane. Il reato contestato dalla Procura Distrettuale è stato di associazione per delinquere finalizzata alla organizzazione e raccolta illegale di gioco di azzardo online. Il gruppo gestiva un giro d'affari di svariati milioni di euro al mese.

Le criptovalute introducono dei sistemi di pagamento svincolati dai sistemi bancari tradizionali e possono portare ad attività di riciclaggio di denaro proveniente da attività criminose. Come vi state muovendo in questo ambito?

Abbiamo sviluppato molte esperienze e conoscenze in materia di moneta virtuale, riuscendo a stringere rapporti con molte società estere che si occupano delle transazioni, i cosiddetti *"exchange"*. È indubbio che la moneta virtuale, con il sistema attuale, si presta ad essere utilizzata nell'ambito del cybercrime così come per le attività di riciclaggio. Di recente, dopo complesse e sofisticate indagini, siamo riusciti a ricostruire la "catena di blocchi" (la cosiddetta *"blockchain"*) e individuare e sequestrare il conto deposito di criptovalute dove si trovavano i proventi illeciti di un falso trading online, identificando gli autori in un cittadino macedone e un albanese.

Pedofilia online, grooming, sextorsion... La lotta all'abuso sessuale online a danno di minori è tra le vostre priorità. Ci può parlare di questo fenomeno e degli strumenti che utilizzate per contrastarlo? Come si può portare la cultura della legalità tra i giovani?

Il contrasto e la prevenzione dell'abuso sessuale online sono, senza dubbio, tra i compiti prioritari

della Polizia di Stato. Le varie condotte legate alla pornografia minorile e gli adescamenti online, in particolare negli anni della pandemia, sono aumentati sensibilmente, e il fenomeno non è certamente in diminuzione. La Polizia Postale ha, a riguardo, validi strumenti di contrasto, tra cui la possibilità di svolgere attività investigative *"sotto copertura"*, ovvero interdire la visione dei siti che diffondono pornografia minorile aggiornando costantemente una *"black list"*. In particolare, attraverso il Centro Nazionale per il contrasto della pedopornografia online, la Polizia Postale raccoglie segnalazioni, provenienti sia da altre Forze di Polizia, anche straniere, sia da cittadini, da associazioni di volontariato e da provider, coordina le indagini a livello nazionale e stila le black list dei siti web pedofili. Ma un efficace contrasto del fenomeno passa anche dalla sensibilizzazione dei minori sui rischi online. Abbiamo l'assoluta convinzione che il modo migliore per un efficace lotta dei crimini sia la prevenzione e, certamente, essa deve partire dai più giovani. Per questo, come Polizia di Stato, siamo quotidianamente impegnati in incontri con gli studenti, partendo dalla scuola primaria fino alle superiori, ma anche con gli insegnanti e i genitori che spesso non hanno consapevolezza dei gravi rischi in cui possono incorrere i loro figli. E proprio loro, i genitori, devono rappresentare il primo baluardo di difesa.

La *"rete"* amplifica le conseguenze dei reati che rimangono visibili anche dopo avere scontato la condanna. Ci può parlare del diritto all'oblio e di come questo può essere esercitato?

Il diritto all'oblio è *"il diritto di essere dimenticati"*. Mentre il Gdpr (Regolamento UE n. 679/2016 sulla protezione dei dati personali) con l'art. 17 lo prevede come il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, in generale è considerato, tuttavia, come il diritto di ciascuna persona affinché un'informazione che lo danneggia sia eliminata, in particolare se riguarda un fatto molto risalente nel tempo. È un diritto riconosciuto dall'ordinamento giuridico, ad esempio previsto anche dalla legge 71/17 sul cyberbullismo, e che consente di rivolgersi direttamente ai gestori del contenuto o al Garante della Privacy chiedendo la cancellazione del dato che si ritiene lesivo. Occorre evidenziare, tuttavia, che ha una difficile applicazione pratica perché alcuni servizi della Rete, come ad esempio l'ubicazione del dato in server esteri, non rendono semplice la sua eliminazione, aggiungendo che una informazione veicolata, ad esempio, tramite i servizi di messaggistica, risiede in tutti i dispositivi che l'hanno gestita con relative difficoltà a eliminarla.

Per concludere, ci può raccontare un caso difficile ma che ha chiuso con successo? Quali sono le prossime sfide che attendono lei e il suo reparto?

Nella vita professionale di un poliziotto sono tanti i casi difficili che egli deve affrontare. Certamente di alcuni rimane un maggior ricordo, magari per motivi che non riguardano solo la complessità delle indagini ma anche gli aspetti umani, a maggior ragione quando si tratta di reati concernenti lo sfruttamento sessuale di minori. Tra le tante indagini di questo tipo vi è l'operazione nota come *"12 Apostoli"*, una investigazione complessa che ha messo in luce l'esistenza di un'associazione a delinquere finalizzata alla violenza sessuale aggravata ai danni di minori. Il futuro delle nostre attività abbraccia sfide sempre più importanti e impegnative, in un mondo in cui la tecnologia e la rete hanno ruoli determinanti nel nostro vivere quotidiano. Basti pensare al progredire dell'utilizzo dell'Intelligenza Artificiale e del cosiddetto Internet delle Cose. La Polizia, in questo contesto, deve continuare a garantire la sicurezza dei cittadini, delle imprese e della collettività.

Chi è Marcello La Bella

Primo Dirigente della Polizia di Stato, **Marcello La Bella** è attualmente dirigente del **Centro Operativo Sicurezza Cibernetica "Sicilia Orientale"**. Già componente del gruppo di lavoro ministeriale per la creazione del Polo Sicurezza Cibernetica, ha lavorato presso uffici investigativi quali Digos e Squadra Mobile. Ha esperienze d'indagine nei settori della criminalità organizzata, dei reati informatici e delle pornografia minorile su Internet. Ha frequentato corsi internazionali e preso parte, quale rappresentante della Polizia italiana, a numerosi convegni e a gruppi di lavoro, in Italia e all'estero, in materia di criminalità informatica e pedopornografia.

Quando si dice *"il caso"*

Entrare nel mondo della sicurezza e poi, grazie a un caso in particolare, diventare uno degli investigatori privati più noti e apprezzati sulla scena nazionale e non solo. È la storia di Marco Gallo, oggi vicepresidente Area Sud di Federpol, detective con un'esperienza trentennale e un amore per la propria professione che il tempo non ha scalfito.

di Virna Bottarelli

Quella di intraprendere la carriera dell'investigatore privato è stata, per **Marco Gallo**, vicepresidente Area Sud di **Federpol**, una scelta *"nata per caso"*. Sono i primi anni Novanta e Gallo, non ancora trentenne, si avvicina al mondo della sicurezza: *"In quegli anni iniziai a capire che cosa volesse dire fare un'analisi dei rischi, a livello di sicurezza industriale e di sicurezza delle persone"*, racconta ripercorrendo i suoi primi anni di lavoro. *"Inizialmente il mio obiettivo era lavorare come guardia del corpo, ma una volta appurato che si trattava, e si tratta, di una figura professionale non giuridicamente riconosciuta nel nostro Paese, mi sono orientato verso le investigazioni"*. I primi anni non sono facili perché, come spiega Gallo, *"non fu facile farsi accettare e riconoscere come professionista sul mercato della sicurezza industriale, soprattutto nel Sud Italia, dove operavo"*, ma dopo qualche collaborazione con agenzie investigative in diverse città italiane, nel 1995 Gallo avvia la propria attività e, proprio in quell'anno assume un mandato di investigazione per un caso di cronaca nera a cui ancora oggi è associato il suo nome: la scomparsa di **Elisa Claps**.

Ci racconta come arrivò a seguire il caso di Elisa Claps e come contribuì, con le sue ricerche, ad accertare quanto accaduto alla giovane?

Conobbi la madre di Elisa Claps, **Filomena**

Iemma, casualmente, in occasione di un convegno. La storia della scomparsa della figlia, avvenuta il 12 settembre 1993, e le difficoltà incontrate dalla famiglia nel convincere le autorità competenti ad approfondire le indagini sul caso mi colpirono molto e mi indussero a offrire loro, a titolo gratuito, la mia consulenza. Quello conferitomi dalla famiglia di Elisa, nel novembre 1995, fu il primo mandato ricevuto dalla mia agenzia: impiegai due anni per raccogliere tutti gli elementi utili a formarmi un'idea sul caso, intervistando le persone più vicine a Elisa, amici e conoscenti che la frequentavano a Potenza, fino ad arrivare alla Chiesa della Santissima Trinità, che però non ho mai potuto ispezionare per i divieti imposti dal parroco dell'epoca, Don Domenico Sabia. Per tutto il periodo di investigazioni tenni informata la polizia dando indicazioni rilevanti: avevo scoperto, ad esempio, che **Danilo Restivo**, l'uomo sul quale convergevano i principali sospetti per la scomparsa di Elisa, e che poi si accertò esserne l'assassino, si era trasferito a Bournemouth e, quando proprio in quella città fu barbaramente assassinata e mutilata **Ether Barnett** non esitai, insieme a **Gildo Claps**, fratello di Elisa, a comunicare alla polizia inglese che Danilo Restivo viveva di fronte alla casa della vittima. Le nostre indicazioni, però, rimasero inascoltate e le indagini ebbero una svolta solo nel marzo 2010, quando, in fondo al sottotetto della Chiesa della Santissima Trinità, alcuni operai durante lavori di ristrutturazione trovarono i resti di Elisa.

E proprio dal ritrovamento del cadavere di Elisa emergeranno altri elementi a infittire il mistero di un caso rimasto irrisolto per diciassette anni...
Ebbi la possibilità di documentare scrupolosamente la scena del ritrovamento, al quale lavorarono, su indicazione della Procura, gli esperti della Polizia Scientifica e del Ris. Un dettaglio mi colpì in particolare: sul corpo di Elisa furono rinvenuti, intatti, alcuni semi di un albero di acacia che normalmente volano nell'aria nei mesi di settembre e ottobre. Come potevano essersi depositati sul cadavere e non essersi decomposti se il corpo fosse stato da anni ricoperto da calcinacci e materiale di risulta? Era molto probabile che il corpo fosse stato scoperto almeno sei mesi prima di quel 17 marzo 2010, se non un anno e sei mesi prima di quella data. Svolsi quindi nuove indagini in loco, parlando con i negozianti della zona. In particolare, una commerciante riferì che circa un anno e mezzo prima aveva denunciato alcuni vandali che si erano serviti di materiale di risulta scaricato dal tetto della Chiesa e appoggiato in strada in attesa di essere smaltito per spaccare la vetrina del suo negozio. Grazie alla denuncia risalimmo alla data del fatto, trovammo chi, in quel periodo, si era occupato di portare a

Il caso Claps

Elisa Claps, una studentessa di sedici anni, scompare a Potenza il 12 settembre 1993. Il suo cadavere è rinvenuto solo il 17 marzo del 2010 nel sottotetto della Chiesa della Santissima Trinità, in occasione di alcuni lavori di ristrutturazione dell'edificio. Le indagini successive appurano che ad assassinare la ragazza è stato, il giorno stesso della sua scomparsa, **Danilo Restivo**, all'epoca dei fatti ventunenne. Restivo è stato giudicato colpevole anche dell'omicidio di Heather Barnett, compiuto nel 2002 in Inghilterra.

VUOI DIVENTARE INVESTIGATORE E CRIMINOLOGO?

SCEGLI TRA:

- CORSO DI LAUREA IN SCIENZE GIURIDICHE PER LA CRIMINOLOGIA, L'INVESTIGAZIONE E LA SICUREZZA
- CORSO DI ALTA FORMAZIONE IL CRIMINOLOGO PROFESSIONISTA

EI POINT FEDERPOL
unimercatorum@federpol.it

FEDERPOL · FEDERAZIONE ITALIANA ISTITUTI INVESTIGAZIONI · INFORMAZIONI · SICUREZZA

Università Mercatorum
Università telematica delle Camere di Commercio Italiane

terra il materiale di risulta e informammo il PM **Rosa Volpe**. La procura avviò così nuove indagini sulle imprese delle pulizie che frequentavano la Chiesa in quel periodo e sui parroci che, dopo la morte di don **Domenico Sabia**, avvenuta nel marzo 2008, avevano in gestione la parrocchia. Arrivai alla conclusione che il Vescovo di Potenza, **Agostino Superbo**, e don **Ambroise Atakpa**, parroco della Santissima Trinità, furono determinanti nel far ritrovare il cadavere di Elisa, ma mentirono sulla data del ritrovamento.

Ci sono stati altri casi altrettanto impegnativi ai quali ha dato il suo contributo come investigatore?
Ho lavorato a diversi casi, ma ne cito due in particolare che ricordo come significativi. Uno riguardava un caso di presunto omicidio poi rivelatosi suicidio, sul quale ebbi la fortuna di lavorare in collaborazione con il compianto professor **Andrea Antonio Dalia**, autore dell'omonimo manuale di procedura penale. Fu un caso complesso, al quale lavorammo a distanza di vent'anni dall'accaduto. Una seconda esperienza degna di nota risale invece al 2014, quando fui incaricato di lavorare al caso, internazionale, di una bambina sottratta alla madre dal padre, un cittadino siriano, che era riuscito a portare la figlia di nemmeno due anni oltreconfine, eludendo i controlli di frontiera all'insaputa della madre, dalla quale si era recentemente separato. Una vicenda complicata, per la quale mi sono recato in Turchia, per pedinare il soggetto, facendomi supportare da un collaboratore che, conoscendo l'arabo, ha potuto colloquiare con lui senza destare sospetti, e che si è conclusa solo nel 2017 con il rientro della bambina in Italia e la condanna del padre per sequestro di persona e sottrazione di minore.

In una intervista rilasciata a Federpol Mag due anni fa, lamentava il fatto che all'investigatore privato non fosse riconosciuta l'autorevolezza che merita. Oggi direbbe la stessa cosa o qualcosa è cambiato negli ultimi tempi?
Oggi, c'è sicuramente una maggiore consapevolezza da parte delle Istituzioni dell'importanza del nostro ruolo e della nostra professionalità. Lo stereotipo del detective sopra le righe, del personaggio ai limiti della legalità, si è indebolito molto negli ultimi tempi. A questo ha senza dubbio contribuito l'attività di Federpol, con la certificazione universitaria dei nostri corsi di formazione, che ha rappresentato un passaggio fondamentale, recepito anche dal Decreto Ministeriale del 2010: la norma stabilisce il requisito, per chi volesse intraprendere la nostra professione, di una preparazione e di un aggiornamento di qualità. Un altro passaggio importante è stato il rilascio del tesserino ministeriale, che oggi ci consente di essere riconosciuti anche formalmente come professionisti e di accedere a piattaforme di dati prima a noi precluse.
Infine, il 18 gennaio 2023, la categoria ha compiuto un altro importante passo con la firma dell'intesa con la **Scuola Superiore dell'Avvocatura**: l'intesa favorisce una sinergia con gli avvocati e ci consente di contribuire al miglioramento delle normative. Si tratta di un tassello significativo anche per il percorso volto a garantire quel giusto processo che, sebbene previsto dal nostro ordinamento, è ancora ben lontano dall'essere effettivamente tradotto in realtà.

Che cosa, invece, non è cambiato dagli inizi della sua carriera a oggi?
Un punto fermo è l'amore per la professione. È ciò che mi spinge, ancora oggi che ho 59 anni e un bagaglio consistente di esperienza alle spalle, a studiare nei dettagli ogni caso che affronto e ad aggiornarmi per essere un professionista preparato e affidabile.

Chi è Marco Gallo

Salernitano, 59 anni, **Marco Gallo** ha un'esperienza trentennale come investigatore. Membro e socio **Federpol** dal 2003, è Vicepresidente Sud della Federazione. Detective Professionista, esperto in Sicurezza Aziendale e Personale, Investigazioni Civili e Penali, Grafologia e Balistica, è anche ambasciatore per l'Italia della **World Association of Detective** e socio onorario dell'associazione nazionale **San Giuseppe Moscati**, dedicata alla lotta all'usura.

Avvocato e investigatore: due professionisti, una verità

Il protocollo d'intesa siglato da Federpol e dalla Scuola Superiore dell'Avvocatura rappresenta una tappa importante nel percorso di riconoscimento formale della professione, e della professionalità, degli investigatori privati. Come si è arrivati a questo traguardo? E in che modo la collaborazione tra avvocati e detective può contribuire a migliorare la ricerca della verità e il perseguimento della giustizia?

di Virna Bottarelli

Il 18 gennaio 2023 a Roma è stato siglato il Protocollo d'intesa tra la **Scuola Superiore dell'Avvocatura** e **Federpol**. La firma è il risultato dell'impegno da tempo profuso dall'associazione nel dare alla professione dell'investigatore un adeguato riconoscimento in termini, appunto, di professionalità e competenza.

Come ha detto il presidente **Luciano Tommaso Ponzi**: *"La firma del protocollo d'intesa con la Scuola Superiore dell'Avvocatura significa tanto, non solo per il suo importante contenuto, ma anche per ciò che rappresenta. Uno stereotipo culturale sbagliato, retaggio del passato, unitamente a una scarsa conoscenza della nostra professione da parte soprattutto dei mass media, infatti, finisce spesso per ghettizzare la figura dell'investigatore privato, fornendone una definizione assolutamente inappropriata, sicuramente fuorviante, oserei dire quasi offensiva, lesiva di un'intera categoria. La qual cosa avviene anche da parte di esperti o asseriti tali che vengono chiamati quali opinionisti nelle varie trasmissioni e ci dipingono come faccendieri o facili risolutori di problematiche borderline"*. Come è stato più volte spiegato proprio dalle pagine di Federpol Mag, invece, e come ribadisce lo stesso Ponzi, l'investigatore privato *"oggi si occupa di controspionaggio industriale, tutela del patrimonio, fa da consulente tecnico di parte in giudizio, utilizza tecnologie all'avanguardia, è di ausilio agli avvocati nella ricerca della verità processuale"*. Oltre che essere un traguardo, il Protocollo d'Intesa è anche un punto di partenza per una serie di attività di formazione, consulenza e studio di norme, come sottolinea **Stefano Cimatti**, Presidente del Comitato per la Formazione di Federpol. *"Negli ultimi anni ci siamo aperti a collaborazioni con il mondo delle professioni e, in generale, delle istituzioni, dalle prefetture, alle questure, alle amministrazioni pubbliche"*, ha detto Cimatti, *"perché in un mondo come quello odierno, così differenziato per singole specialità, è cruciale avere un'interlocuzione continua con i tanti soggetti che gravitano nel nostro contesto professionale"*.

Una sinergia a vantaggio delle due categorie

La Scuola Superiore dell'Avvocatura è una fondazione del **Consiglio Nazionale Forense**, che esercita le proprie funzioni in linea con le finalità che la legge attribuisce a quest'ultimo in materia di formazione, aggiornamento e attività scientifiche e culturali relative alla professione di avvocato. La presiede l'avvocato **Maria Masi**, mentre alla vicepresidenza siede l'avvocato **Giovanna Olla**. Proprio quest'ultima, in occasione della firma della convenzione, ha precisato come il ruolo dell'investigatore privato nel contesto del processo penale sia definito dalla riforma delle investigazioni difensive, che risale al 2001, e dall'articolo 391 bis del Codice di procedura penale. *"Queste disposizioni hanno attribuito all'investigatore un ruolo importante nella ricerca della prova nell'ambito del processo penale, nell'interlocuzione dialogica con le persone informate sui fatti e, ancora prima, nella ricerca dei soggetti che possono essere informati sui fatti e che quindi possono dare un contributo alla ricerca della prova"*.
Stefano Bertollini, del Consiglio Nazionale Forense, ricorda come la collaborazione tra le due categorie sia necessaria, perché gli avvocati sono per gli investigatori degli *"interlocutori naturali nello svolgimento delle attività di investigazione"* e perché è fondamentale per gli avvocati *"implementare la conoscenza delle attività condotte dagli investigatori privati nel contesto professionale forense, a maggior ragione perché la loro figura è spesso trascurata nelle aule di giustizia"*. Il punto è diffondere la conoscenza delle potenzialità che gli investigatori hanno e di come la loro competenza può essere di supporto agli avvocati: *"Siamo in un mondo dove la specializzazione la fa da padrona"*, dice ancora Bertollini, *"e non possiamo pensare, come avvocati, di sostituirci a degli esperti in materie che non rientrano nelle nostre competenze. Inoltre, siamo in un'epoca di rapidi cambiamenti e siamo chiamati a tenerne il passo: questa collaborazione è una bella occasione per i nostri iscritti, ai quali possiamo offrire nuove opportunità di formazione e conoscenza"*.
La relazione tra avvocati e investigatori non si limita però alle aule di giustizia. Gli avvocati svolgono anche attività consulenziali nell'ambito, ad esempio, della crisi d'impresa e della contrattualistica, o, ancora, siedono negli organismi di vigilanza. Per questo, come spiega **Milène Sicca**, presidente del Comitato Studi Legislativi di Federpol, *"hanno bisogno di confrontarsi con gli investigatori, proprio per acquisire quegli elementi che servono per capire quale sia il rischio, incombente e prospettico, in cui può incorrere l'impresa"*. La sinergia tra avvocato e investigatore diventa quindi strategica *"per abbattere le asimmetrie informative, ossia le distanze tra situazioni apparenti e situazioni reali, e, sulla base di una conoscenza certa, intraprendere in modo consapevole azioni che altrimenti sarebbero azzardate"*.

I contenuti dell'intesa

La Scuola Superiore dell'Avvocatura e Federpol si impegnano, siglando il Protocollo d'Intesa, a realizzare azioni comuni per promuovere e incentivare iniziative di informazione sulla figura dell'investigatore privato, valorizzandone i punti di forza, attraverso lo svolgimento di specifici eventi di orientamento rivolti ai diversi operatori della giurisdizione, e a fare attività di formazione per gli avvocati e gli investigatori privati muniti di licenza. Non ultima, la promozione comune e condivisa di interventi legislativi migliorativi dell'attuale assetto normativo che riguarda la categoria. L'idea di fondo della collaborazione è di sviluppare in sinergia le competenze, con l'obiettivo di ricercare verità e giustizia. Tra le attività che le parti si impegnano a intraprendere vi sono anche tavoli di lavoro di tipo tecnico-scientifico per lo studio di tematiche attinenti la professione dell'investigatore titolare di licenza, anche per proporre interventi normativi in materia e la modifica di norme vigenti.

La parola all'avvocato Eraldo Stefani

"Da molti anni auspicavamo una collaborazione tra investigatori privati e avvocati e finalmente, con questo protocollo di intesa, abbiamo compiuto un passo concreto in questa direzione", dice il professor **Eraldo Stefani**, avvocato e consulente di Federpol per le indagini difensive.

Avvocato Stefani, da anni segue le attività di Federpol. Come si è evoluto nel tempo il rapporto tra avvocati e investigatori privati?
È un rapporto che è andato migliorando, va detto, in gran parte per merito di Federpol, che ha fatto un percorso importante nell'avvicinare le due professioni e nell'organizzare diversi momenti formativi.

Nella sua esperienza, ci sono stati casi nei quali la collaborazione con un investigatore privato è stata cruciale nella tutela di un suo assistito?
Senza dubbio. Ricordo, in particolare, il caso di un duplice omicidio, nel 2001, al quale contribuì in modo determinante un investigatore privato. Fece un ottimo lavoro individuando una persona informata sui fatti, che non era stata sentita dall'autorità giudizia-

ria, ma che poteva portare degli elementi determinanti per provare la non colpevolezza dell'imputato. Nel processo gli elementi furono riconosciuti come prove dell'innocenza di quest'ultimo, che fu poi assolto. È un esempio di come l'investigatore privato con esperienza possa portare un contributo importante alle indagini. Potrei azzardare una sorta di similitudine: l'investigatore riveste per l'avvocato il ruolo che la Polizia, i Carabinieri e la Guardia di finanza ricoprono per il Pubblico Ministero.

Avvocato e investigatore agiscono, quindi, in sinergia. Ma c'è ancora qualche divergenza da smussare nel rapporto tra queste due figure professionali?
Fino a qualche anno fa c'era una certa diffidenza reciproca: da un lato gli investigatori pensavano che gli avvocati non tenessero in giusta considerazione la loro figura, dall'altro, effettivamente, gli avvocati non reputavano l'attività degli investigatori utile nell'accertamento della verità. Con il tempo queste posizioni si sono indebolite e oggi è riconosciuto che l'investigatore privato è un professionista importante, il cui ruolo in ambito penale è insostituibile.

Può spiegarci perché la Riforma Cartabia ha dei risvolti che interessano l'attività degli avvocati e, di riflesso, quella degli investigatori privati?
La Riforma Cartabia ha posto una condizione per i casi in cui si effettua una verbalizzazione delle dichiarazioni della persona informata sui fatti: l'avvocato, oltre che alla verbalizzazione, deve provvedere anche alla registrazione totale della stessa. Si tratta di un aspetto che riguarda pariteticamente anche il Pubblico Ministero, la Polizia, i Carabinieri e la Guardia di Finanza e che a mio avviso va accolto con favore, perché allontana lo spettro dell'errore giudiziario. La registrazione consente infatti di produrre prove documentali importantissime per il processo penale. C'è un aspetto critico, però, da tenere presente: la Riforma prevede che nel caso vi sia una problematica contingente, ossia non vi sia nessun dispositivo disponibile per la registrazione, quest'ultima non sia necessaria. Mi auguro non si diffonda questa prassi e che si proceda sistematicamente alla registrazione dei verbali: del resto, è sufficiente avere uno smartphone per poterla avviare.

C'è un altro aspetto della Riforma Cartabia, che lei ha recentemente sottolineato, sostenendo che essa lascia agli avvocati molti spazi di iniziativa. In che senso?
Con la riforma, l'avvocato ha un ampio margine d'azione nella sfera della giurisdizione privata, ed è proprio in questo ambito che anche l'investigatore può avere un ruolo determinante. L'idea è che molte controversie, soprattutto per quanto riguarda le attività di impresa, possano essere risolte evitando di dover ricorrere ai tribunali. Un bravo avvocato, al pari di un bravo investigatore privato, è colui che supporta l'impresa nell'agire in modo da non incorrere in reati che ne comportino la responsabilità amministrativa e penale ai sensi del D.lgs. 231/2001. Insieme, avvocati e investigatori privati, facendo leva sulla loro professionalità, possono assistere le imprese in modo da prevenire ed eventualmente correggere eventuali criticità nei loro modelli organizzativi e nel loro modo di operare.

Che cosa cambierà in futuro grazie alla firma del protocollo di intesa tra Federpol e Scuola Superiore dell'Avvocatura?
Oltre a rinsaldare il rapporto tra le due categorie, l'intesa servirà a colmare delle lacune importanti che, anche personalmente, ho riscontrato nella conoscenza da parte dell'investigatore privato degli obblighi di rispetto e fedeltà derivanti dal rapporto di collaborazione con un avvocato. Un esempio su tutti: è accaduto che investigatori privati rilasciassero informazioni ai media senza l'autorizzazione degli avvocati con cui stavano lavorando al caso. Errori di questo tipo, gravi perché possono inficiare il corso delle investigazioni e anche perché violano le limitazioni imposte dalle normative sul rispetto della privacy, non dovrebbero più essere commessi se c'è una conoscenza puntuale dei diritti e dei doveri inerenti al rapporto professionale tra investigatore e avvocato.

Eraldo Stefani, avvocato e consulente di Federpol per le indagini difensive

Responsabilità civili dell'investigatore privato: che cosa c'è da sapere

Le "cattive investigazioni" o il "cattivo utilizzo delle investigazioni" possono generare ipotesi di responsabilità civile per l'investigatore privato e comportare l'obbligo di risarcimento del danno. Per evitare tale eventualità, è fondamentale conoscere le norme di riferimento e operare entro i limiti consentiti.

di Alessandro Barca

L'investigatore privato non è solamente un testimone diretto di quanto accade sotto i propri occhi, ma ha anche la possibilità di deporre davanti al giudice sui fatti a propria conoscenza. Affinché i frutti delle indagini dell'investigatore privato possano costituire prova testimoniale all'interno di un giudizio, è necessario che le dichiarazioni di questi vengano acquisite mediante prova orale o testimonianza scritta (art. 257 bis c.p.c.). Se si vuole che la relazione dell'investigatore assuma carattere testimoniale, non è sufficiente che la prova orale confermi in blocco il contenuto del documento/relazione dello stesso investigatore, ma è necessario che l'investigatore sia in grado di narrare fatti precisi, circostanziati e chiari, che abbia appreso con la sua percezione diretta. Nel caso di foto e video, qualora non possano giungere (perché, ad esempio, contestati) a formare il convincimento del Giudice, la prova può essere raggiunta con la deposizione dell'investigatore. Questi, infatti, in quanto osservatore oculare dei fatti a cui ha assistito è, come detto, anche testimone. Dunque, egli potrà confermare verbalmente al giudice ciò che ha visto; le sue dichiarazioni, in questo modo, andranno ad avvalorare anche il materiale video raccolto per superare eventuali contestazioni di controparte.
La giurisprudenza ha affermato *(Cass., n. 18131/2004; Cass. n. 12763/2000; Cass., n. 8/2000; Cass. n. 4821/1999)* che i rapporti scritti degli investigatori privati, fuori dai casi in cui assumono il valore di prova testimoniale, sono da considerarsi prove atipiche a tutti gli effetti. In particolare, sono da considerarsi *"scritti del terzo"* redatti in funzione testimoniale su incarico di parte e prova atipica avente il valore di presunzione semplice ex art. 2729 c.c. o di argomento di prova. Il ruolo dell'investigatore, dunque, è compresso tra l'attività di investigazione e l'utilizzo delle sue relazioni investigative dentro il processo e fuori dal processo. Le *"cattive investigazioni"* o il *"cattivo utilizzo delle investigazioni"* può generare ipotesi di responsabilità civile per l'autore delle medesime.

Norme di riferimento

Per evitare di incorrere in ipotesi di responsabilità civile e conseguente obbligo di risarcimento del danno è importante per l'investigatore privato conoscere a fondo la normativa in materia di privacy e protezione dei dati personali. I riferimenti normativi di cui tenere conto sono i seguenti:

- **Articolo 2 della Costituzione |** Colloca la persona al centro rispetto ai controlli dello Stato e riconosce la persona come titolare di diritti inviolabili che la Repubblica riconosce, tutela e garantisce.
- **Articolo 2043 Codice civile: "qualunque fatto che cagioni ad altri danno ingiusto obbliga colui che l'ha commesso a risarcire il danno" |** Disciplina il sistema della responsabilità civile/illecito. Se in sede di attività investigativa si rispettano i principi riportati, non si incorre in alcuna ipotesi di responsabilità civile.
- **Regolamento UE 679/2016 sulla protezione dei dati personali (cosiddetto Gdpr) |** Nell'attività investigativa occorre procedere con un attento utilizzo delle nozioni di "dato personale" (qualsiasi informazione riguardante un individuo identificato o identificabile con una formulazione volutamente generica; comprende al proprio interno un'ampia serie di dati relativi agli individui, tra cui i più comuni sono nome, cognome, codice fiscale, numero di telefono, indirizzo e-mail, ma anche fotografie e video quando il soggetto è identificabile e anche, quindi, nei casi in cui sia possibile risalire all'identità della persona ritratta combinando l'immagine con altri elementi identificativi); "trattamento" dei dati (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, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione). L'articolo 5 del Gdpr stabilisce come deve avvenire il trattamento dei dati personali: è necessario effettuare operazioni lecite, corrette, trasparenti, ridotte al minimo e per finalità predefinite e specifiche; i dati devono essere conservati per il tempo strettamente necessario per raggiungere le finalità e deve esserne sempre assicurata l'esattezza, l'integrità e la riservatezza, oltre che il costante aggiornamento; tali modalità di trattamento devono favorire in concreto il rispetto dei diritti, delle libertà e della dignità dei soggetti interessati, ossia delle persone fisiche/giuridiche cui i dati sono riferiti; è necessario integrare i principi dettati dal Gdpr nelle proprie prassi operative.
- **Regole deontologiche per il trattamento a fini di archiviazione, pubblicate dal Garante per la protezione dei dati personali il 19 dicembre 2018 e in vigore dal 2019 |** Si applicano al trattamento dei dati personali non solo in presenza di un procedimento giudiziario già instaurato, ma anche nella fase propedeutica e in quella successiva alla definizione dello stesso. In particolare, l'inve-

stigatore non può intraprendere tale attività di propria iniziativa, perché anche questo è fonte di responsabilità civile. All'investigatore deve essere conferito apposito incarico scritto, in cui devono essere menzionati specificamente:

- **il diritto che deve essere esercitato o il procedimento a cui l'investigazione si riferisce;**
- **i principali elementi di fatto che giustificano la richiesta di investigazione e il termine entro cui l'investigatore deve concludere la propria attività;**
- **il carattere personale, o meno, dell'incarico conferito.**

Rispetto a quest'ultimo punto, l'investigatore deve eseguire l'incarico personalmente quando si tratta di un'indagine difensiva, mentre può avvalersi del supporto di altri collaboratori nel caso si tratti di indagini per far valere un diritto in sede giudiziaria. Queste persone saranno quindi autorizzate al trattamento dei dati personali strettamente necessari per l'investigazione e l'investigatore dovrà fornire loro le istruzioni operative e vigilare con cadenza almeno settimanale sul loro operato. Tale obbligo di vigilanza è funzionale anche al rispetto del dovere di informare periodicamente il soggetto che ha fornito l'incarico con riguardo all'andamento delle indagini. Nel momento in cui cessa la specifica attività investigativa, deve, di conseguenza, cessare anche il trattamento. La conservazione ulteriore dei dati personali (art. 10) può essere autorizzata dal soggetto che ha conferito l'incarico al solo fine di dimostrare la liceità, la trasparenza e la correttezza dell'operato dell'investigatore. Finché l'informazione è necessaria per le attività di indagine potrà essere conservata mentre nel momento in cui, anche qualora il procedimento fosse ancora pendente, tale dato non si rivelasse più essenziale per lo svolgimento di quell'incarico, alla luce del principio di minimizzazione e di limitazione della conservazione, il dato dovrebbe essere cancellato.

- **Codice deontologico delle Agenzie Investigative e degli investigatori privati associati alla Federpol |** Il tema della protezione dei dati personali è citato all'articolo 1, dove si legge che tutti gli associati *"si impegnano al rispetto del diritto alla protezione dei dati personali, del diritto alla riservatezza e del diritto all'identità personale"*. Il Codice fa riferimento al Gdpr, nella parte *"Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria"* (ossia regole deontologiche per il trattamento a fini di archiviazione), e alle già citate regole pubblicate dal Garante per la protezione dei dati personali.

Il danno e il suo risarcimento

La norma che riconosce in modo specifico il risarcimento del danno conseguente a un illecito trattamento dei dati personali è l'articolo 82 del Gdpr: chiunque subisca un danno materiale o immateriale causato da una violazione del Gdpr ha diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento. Un trattamento di dati personali è illecito se non è conforme al Gdpr (art. 82) e/o agli atti delegati e agli atti di esecuzione adottati in conformità al Gdpr (ad esempio, Codice della privacy) e alle disposizioni nazionali che specificano disposizioni contenute nel regolamento (considerando l'art. 146 del Gdpr). Si tratta, ad esempio, delle condotte che violano i cosiddetti atti di *"soft law"*, come i provvedimenti e le autorizzazioni generali del Garante privacy.
Tra le ragioni che possono essere poste alla base di una richiesta di risarcimento vi sono (considerando l'art. 85 del Gdpr):

- **perdita del controllo dei dati personali degli interessati;**
- **limitazione dei loro (degli interessati) diritti;**
- **discriminazione;**
- **furto o usurpazione d'identità;**
- **perdite finanziarie;**
- **decifratura non autorizzata della pseudonimizzazione;**
- **pregiudizio alla reputazione;**
- **perdita di riservatezza dei dati personali protetti da segreto professionale.**

La prova dell'evento dannoso, del danno che ne è conseguito e del nesso causale deve essere fornita da colui che richiede il risarcimento. Il danno astrattamente risarcibile è sia quello patrimoniale che quello non patrimoniale. Il primo consiste in perdite economiche o finanziarie se talune raccolte di dati in determinate circostanze vengono poi utilizzate o riutilizzate in circostanze diverse (ad esempio, profilazioni di merito non aggiornate o non adeguatamente realizzate, che possono influire negativamente in una selezione professionale per determinate mansioni oppure nell'ottenimento di un finanziamento bancario sul piano del merito creditizio); il secondo, detto anche danno morale, perché lede diritti costituzionalmente protetti, consiste nella lesione di interessi inerenti la persona, non connotati da rilevanza economica (ad esempio, lesione identità, onore, riservatezza, immagine, decoro, dignità dell'essere umano).

Svolgere l'attività investigativa in modo corretto

Entro quali limiti, allora, può agire l'investigatore privato per non incorrere in una ipotesi di responsabilità civile/con conseguente obbligo di risarcimento del danno? Le casistiche sono diverse per i diversi ambiti di attività dell'investigatore e di seguito riportiamo solo qualche spunto. In linea generale, l'investigatore privato non può violare la riservatezza altrui (ad esempio, introducendosi in luoghi di privata dimora/abitazione, riprendendo luoghi di privata dimora o carpendo informazioni da e-mail o messaggi telefonici ottenuti tramite software spia). Una prova così acquisita non può essere tenuta in considerazione in un giudizio civile ed è fonte di responsabilità civile.
Nell'ambito delle investigazioni sui lavoratori, va ricordato che l'art. 8 della Legge n. 300/1970 *(Statuto dei Lavoratori)* vieta indagini sui dipendenti anche tramite investigatori privati, salvo che si tratti di illeciti commessi dal lavoratore all'interno dell'azienda, come ad esempio ammanchi inventariali o uscite/assenze ingiustificate dal luogo di lavoro. Lo Statuto stabilisce anche che il datore di lavoro, anche tramite investigatori privati, può effettuare controlli a distanza con altri strumenti (non di lavoro), come impianti audio visivi, ma solo per esigenze organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale e non per verificare l'adempimento della prestazione lavorativa. In ogni caso il datore di lavoro deve informare preventivamente il lavoratore sulle modalità d'uso degli strumenti e sullo svolgimento dei controlli e attenersi alla disciplina della privacy.
Per quanto riguarda le informazioni commerciali, infine, è utile ricordare l'art 5 lett. b) del DM 269/2010, che riporta scopi, contenuti e fonti lecitamente acquisibili per la realizzazione dei rapporti informativi. Parliamo, come indicato dalla normativa, di *"attività, richiesta da privati o da enti giuridici pubblici e privati di raccolta, analisi, elaborazione, valutazione e stima di dati economici, finanziari, creditizi, patrimoniali, industriali, produttivi, imprenditoriali e professionali delle imprese individuali delle società anche di persone, persone giuridiche, enti o associazioni nonché delle persone fisiche, quali ad esempio, esponenti azienda/i, soci professionisti lavoratori; parti contrattuali clienti anche potenziali dei terzi committenti, nel rispetto dello vigente normativa nazionale e comunitaria in materia di tutela della privacy"*.
Per lo svolgimento di queste attività *"i soggetti autorizzati possono, anche a mezzo di propri collaboratori segnalati ai sensi dell'art. 259 del Regolamento d'esecuzione, raccogliere informazioni provenienti sia da pubblici registri elenchi atti o documenti conoscibili da chiunque (visure camerali, visure ipocatastali, bilanci, protesti, fallimenti e procedure concorsuali, certificati o estratti anagrafici) o pubblicamente accessibili a chiunque (elenchi categorici, notizie internet), sia provenienti da fonti private (lo stesso committente, l'interessato ed altri soggetti privati), acquisite e trattate per finalità di natura economica o commerciale ovvero di valutazione sulla solvibilità, affidabilità o capacità economica dell'interessato"*.

Chi è Alessandro Barca

Genovese, classe 1965, **Alessandro Barca** si laurea in Giurisprudenza all'Università della propria città dopo aver conseguito il diploma di maturità classica. Iscritto all'Ordine degli Avvocati di Genova dal 2001, nel 2005 consegue, presso l'**Università di Pisa**, il titolo di "Dottore di ricerca in diritto privato", discutendo la tesi "Il recesso nei contratti del consumatore". Dal 2006 al 2011 è stato Professore a contratto di Diritto dei Consumatori, presso la Facoltà di Giurisprudenza dell'**Università di Milano**. Autore di numerosi articoli e saggi, ha curato l'indice analitico di diverse opere ed è responsabile della redazione delle riviste *"Nuova Giurisprudenza Ligure"* e del *"Notiziario del Consiglio dell'Ordine degli Avvocati di Genova"*, Ordine di cui è stato consigliere dal 2006 al 2019. Dei suoi incarichi più recenti ricordiamo quello di membro, dallo scorso aprile, del "Comitato di indirizzo del Corso di Studio" del Corso di Laurea magistrale a ciclo unico in Giurisprudenza dell'**Università degli Studi di Genova**. Dal 2014 è iscritto all'Albo degli Avvocati Cassazionisti.

Un apporto importante alle strategie difensive

L'investigatore privato può mettere a disposizione dei legali competenze altamente specifiche e strumenti tecnologici avanzati con cui individuare elementi di prova che altrimenti rimarrebbero sconosciuti, e dare un apporto importante alle strategie difensive delle diverse parti processuali, sia nella fase precedente che in quella successiva all'iscrizione della "notitia criminis".

di Calogero Licata

Le indagini difensive sono state introdotte nel nostro ordinamento con la Legge 397/2000 al fine di colmare il gap che da sempre esiste tra pubblica accusa e difesa nella fase delle indagini preliminari. Nonostante il principio di parità delle armi abbia quindi ispirato il legislatore italiano, il Pubblico Ministero e la Polizia Giudiziaria dispongono di poteri certamente maggiori rispetto alle facoltà difensive di cui al titolo VI bis del codice di rito, che consta tra l'altro di poche norme in tale materia.

Questo dato di partenza ci induce a riflettere sull'importanza di adoperare tale strumento, alla luce della centralità della fase delle indagini preliminari all'interno del processo penale, sia che si acceda a un rito alternativo, sia che si prosegua nelle forme del rito ordinario. Nel primo caso, l'intero compendio delle indagini preliminari costituisce l'unico - o quasi - patrimonio conoscitivo del Giudice. Nel secondo, invece, le contestazioni, gli atti irripetibili compiuti e la documentazione acquisita dalla PG e financo i verbali di SIT (mediante contesta-

zione o in caso di impossibilità sopravvenuta ad assumere la testimonianza) transitano nel fascicolo dell'organo giudicante, anche senza il consenso delle parti.

Gli spazi d'intervento per l'investigatore privato

L'art. 327 bis c.p.p. definisce le indagini investigative come le attività compiute dal difensore *"in ogni stato e grado del procedimento, nell'esecuzione penale e per promuovere il giudizio di revisione"* che siano volte *"a individuare elementi di prova a favore del proprio assistito"*. Secondo la citata norma, queste facoltà difensive possono essere esercitate da parte del difensore, del sostituto, degli investigatori privati autorizzati e dei consulenti tecnici quando siano necessarie specifiche competenze. Per quanto attiene al profilo temporale, il legislatore ha dunque previsto notevoli spazi di intervento anche per l'investigatore privato, che agisce per conto della persona offesa o dell'indagato. Prima che penda un procedimento penale, qualora si ritenga di essere stati denunciati, è certamente di indubbia utilità la possibilità di raccogliere elementi di prova a difesa, per esempio nei casi di conflittualità tra coniugi o in ambito lavorativo. A ciò si aggiunge che questa facoltà è riconosciuta anche in ambito di reati societari o fallimentari, non esistendo alcuna preclusione di sorta. Si pensi, a esempio, a un'ipotesi di infedeltà patrimoniale dell'amministratore di una società, ove la prova degli atti compiuti in conflitto di interessi potrebbe ben essere acquisita a mezzo di investigazioni difensive.

L'attività difensiva a seguito di iscrizione della *notizia criminis*

L'ipotesi certamente più frequente è quella dello svolgimento dell'attività difensiva a seguito di iscrizione della notizia criminis, ossia in un momento in cui non è scontato che l'indagato abbia piena cognizione del contenuto della stessa. Più precisamente, durante la fase delle indagini preliminari, la persona offesa ha certamente conoscenza della notizia di reato (ma non degli sviluppi investigativi); l'indagato, tutt'al più, potrà ottenere soltanto delle informazioni in merito all'avvenuta iscrizione del proprio nome e del titolo del reato provvisoriamente ascritto.
L'art. 391 bis, primo comma, c.p.p. attribuisce la possibilità di *"conferire con le persone in grado di riferire circostanze utili ai fini dell'attività investigativa"* non solo ai difensori e ai relativi sostituti, ma anche agli investigatori privati, che possono agire in piena autonomia. In quest'ultimo caso, pur non sussistendo alcun obbligo di verbalizzazione, è sicuramente opportuno procedere a una relazione dettagliata, destinata al difensore. Il secondo comma dell'art. 391 bis c.p.p. annovera tra gli strumenti investigativi anche l'assunzione di informazioni o la ricezione di dichiarazioni. Quest'ultime attività possono essere attuate soltanto dal difensore o da un suo sostituto e non dall'investigatore privato, che non è titolare di alcun potere certificativo. È però possibile che l'investigatore coadiuvi il difensore nell'assunzione di informazioni o nella ricezione di dichiarazioni.
In pendenza del processo penale, l'investigatore - la cui posizione ricalca quella della PG - non può riferire su quanto appreso dal soggetto escusso in nessuna delle ipotesi di cui all'art. 391 bis c.p.p. Secondo la Suprema Corte di Cassazione sussiste un'eccezione in tal senso, per cui: *"le dichiarazioni rilasciate all'investigatore privato, delegato dalla compagnia assicuratrice, dalla persona che assumerà la veste di indagato, hanno natura di confessione stragiudiziale e sono, pertanto, utilizzabili in sede processuale e valutabili secondo le regole del mezzo di prova che le immette nel processo" (Cass. Pen., sez. II, sent. n. 1731, del 21/12/2017).* Tali dichiarazioni possono però essere utilizzate solo in assenza di apposito mandato per lo svolgimento dell'attività investigativa preventiva all'investigatore. *(Cass. Pen., Sez. II, sent. n. 10641, del 25/3/2020).*
Com'è noto, il difensore potrà chiedere che i verbali contenti le dichiarazioni ex art. 391 bis, comma 2, c.p.p. siano acquisiti al fascicolo del dibattimento, solo previo consenso delle parti; tuttavia, potrà sempre utilizzarli per formulare contestazioni nei confronti del teste che riferisce in maniera contrastante con quanto precedentemente affermato.
Bisogna poi ricordare che l'eventuale violazione del segreto, da parte dell'investigatore di quanto riscontrato nel corso della sua attività, è penalmente sanzionata ai sensi dell'art. 379 bis c.p., che punisce chiunque riveli notizie segrete relative a un procedimento penale, apprese per avere partecipato o assistito a un atto dello stesso. Da ciò ne deriva che qualsiasi atto compiuto dall'investigatore nell'esercizio del suo mandato sia coperto da segreto.

Attività e strumenti investigativi

Un'importante attività che certamente può essere ricompresa nell'alveo degli strumenti investigativi è quella "dell'accesso ai luoghi", la cui disciplina è contenuta all'art. 391 sexies c.p.p. Per "accesso ai luoghi" si intende la presa visione di luoghi o l'esecuzione di rilievi tecnici, grafici, planimetrici, fotografici o audiovisivi. Chi procede a tale attività può redigere apposito verbale contenente: data e luogo dell'accesso; le generalità dell'investigatore e delle persone intervenute; la descrizione dello stato dei luoghi e delle cose; l'indicazione degli eventuali rilievi. Inoltre, sarebbe opportuno indicare nel verbale sia il procedimento oggetto dell'attività investigativa e del relativo mandato, sia la sottoscrizione in ogni sua pagina delle persone intervenute. Questa modalità investigativa può essere attuata per gli atti ripetibili e irripetibili. I primi possono essere replicati in qualsiasi momento, i secondi, importando la modificazione delle cose oggetto di valutazione, non possono più essere ripetuti. In caso di atti ripetibili, non è previsto alcun onere particolare, se non quello di consentire la partecipazione del PM o della PG, qualora siano presenti o ne facciano richiesta. Per quanto attiene agli atti irripetibili, l'investigatore deve preventivamente avvisare il difensore, affinché quest'ultimo possa notiziare il PM ai sensi dell'art. 391 decies, comma 3, c.p.p. L'accesso è consentito ai luoghi pubblici e privati. Per i secondi, è necessario l'assenso dell'avente diritto, fatta salva la possibilità che sia il Giudice a dare l'ordine, su richiesta del difensore. Qualora il luogo privato sia un'abitazione o una sua pertinenza, occorre che l'accesso sia indispensabile per accertare tracce o altri effetti materiali del reato.

A differenza della PG, l'investigatore può fornire al cliente gli strumenti per procedere alla registrazione di una conversazione di cui quest'ultimo sia parte. Sul punto, la giurisprudenza di legittimità ha però precisato che non è consentito all'investigatore privato installare mezzi di video registrazione all'interno di una privata dimora, neppure se si ha il consenso del proprietario, volti a ritrarre terzi soggetti, i quali compiano attività di natura non delittuosa, come a esempio intrattenere una relazione extraconiugale. In tal caso, è ravvisabile in capo all'investigatore il reato di interferenze illecite nella vita privata, posto che secondo il citato orientamento: *"chi frequenta un luogo di privata dimora, anche se si tratta della dimora altrui, fa affidamento, appunto, sul carattere di "privatezza" dello stesso e, dunque, agisce sul presupposto che la condotta che in quel luogo egli tiene sarà percepita da coloro che in esso siano stati lecitamente ammessi" (Cass. Pen., Sez.V, sent. n. 9235 dell'8/3/2012).*

Oltre agli strumenti investigativi cosiddetti "tipici", che vengono indicati all'interno del codice, ne esistono altri, "atipici", che consistono - a esempio - in servizi di osservazione o pedinamento e che sono certamente leciti. In merito a queste attività, l'investigatore potrà certamente riferire nel corso del dibattimento, oltre che redigere una relazione per il difensore. In conclusione, le indagini investigative possono dare un grande apporto alle strategie difensive delle diverse parti processuali sia nella fase precedente che in quella successiva all'iscrizione della notitia criminis. In futuro, è auspicabile che i difensori si avvalgano sempre di più della collaborazione dell'investigatore, che può certamente mettere a disposizione competenze altamente specifiche e strumenti tecnologici avanzati, con cui individuare elementi di prova che altrimenti rimarrebbero sconosciuti.

Chi è Calogero Licata

Avvocato penalista catanese, **Calogero Licata** si occupa dell'assistenza e difesa di persone fisiche e giuridiche ai sensi del D.Lgs. 231/2001, con particolare riferimento all'ambito del diritto penale dell'impresa e dell'economia, dei reati contro la persona e il patrimonio, dei reati informatici, dei reati in materia ambientale, nonché in materia di responsabilità professionale medica.
È responsabile della Scuola di Formazione della Camera Penale di Catania ed è docente di diritto e procedura penale presso la Scuola di Specializzazione per le professioni legali dell'Università di Catania e presso la Scuola Forense dell'Ordine degli Avvocati di Catania.

Competenze in azione

L'investigatore privato è oggi un professionista competente e preparato, in grado di collaborare al fianco dell'avvocato in modo sinergico e complementare.

di Rita Iacono

Una strategia difensiva che nasce dalla collaborazione tra un avvocato e un investigatore privato, soprattutto se attuata in fase prodromica l'avvio delle azioni giudiziarie, è nella maggior parte dei casi vincente. Una collaborazione simile, infatti, offre la possibilità di ampliare la rete professionale di entrambe le figure e consente di avere una visione più completa dei casi da affrontare. La combinazione di competenze legali e investigative può offrire quindi un valore aggiunto ai due professionisti e costituire, nella gestione dei casi, un vantaggio competitivo in entrambi i settori. Vediamo perché.

Un supporto importante per l'avvocato

Capita sovente che un cliente si rivolga a un avvocato senza avere nessun tipo di informazione utile sulle parti che si troverà a fronteggiare in giudizio. Approfondire le informazioni prima di affrontare il caso può essere di grande aiuto sia per il legale che per il suo cliente, perché consente di mettere a punto le modalità e gli strumenti con i quali raggiungere l'obiettivo prefissato, oltre che di capire sin da subito se è opportuno o meno dar corso all'attività legale. L'avvocato quindi, per svolgere il lavoro in modo efficace, si trova di fronte alla necessità di raccogliere prove, intervistare testimoni o cercare indizi, ed è proprio in questo ambito che entra in gioco il ruolo dell'investigatore privato. Svolgendo indagini sul campo, l'investigatore può consentire al legale con cui collabora di ottenere prove solide, corredate di materiale fotografico e di una relazione minuziosa, in grado di supportare le argomentazioni sostenute dal legale e, in definitiva, di difendere il cliente nel modo più efficace e proficuo possibile.

Un'occasione di crescita per entrambe le categorie

Un investigatore che voglia essere di supporto per la categoria degli avvocati deve essere competente e preparato. Vero è che per poter ottenere il rilascio della licenza dalla Prefettura competente, occorre che il richiedente abbia requisiti di professionalità e di esperienza ben precisi, così come previsto dal D.M. 269/2010, ma è necessario e consigliabile un costante e scrupoloso aggiornamento in materia, da attuare mediante la partecipazione ai corsi di aggiornamento professionale organizzati. A tal proposito occorre ricordare la firma, il 18 gennaio scorso, del Protocollo d'Intesa tra la **Scuola Superiore dell'Avvocatura** e **Federpol**. L'accordo tra le due categorie di professionisti prevede la realizzazione di iniziative di informazione per valorizzare i punti forza dell'investigatore come strumento di supporto all'attività forense, mediante la creazione di eventi specifici e percorsi formativi che saranno aperti, oltre che agli avvocati, anche agli investigatori muniti di regolare licenza. Agli Avvocati che parteciperanno in presenza verranno riconosciuti cinque crediti formativi ai sensi del regolamento sulla Formazione continua approvato dal Consiglio Nazionale Forense.

Chi è Rita Iacono

Laureata in Giurisprudenza e abilitata alla professione forense, **Rita Iacono**, nata e cresciuta a Roma, è titolare di licenza investigativa rilasciata dalla Prefettura della Capitale. Figlia d'arte, ha conseguito una specializzazione in criminologia, scienze forensi e analisi del crimine. Si occupa di consulenza strategica legale e investigativa per aziende e privati. corporate intelligence, compliance management, governance del rischio e innovation management.

Il testimone IoT: quando l'Internet of Things entra nel processo penale

É realmente possibile consentire a uno smart device, o più in generale a un prodotto IoT, di testimoniare in un processo penale, consentendogli di raccontare come si sono svolti i fatti che sono oggetto di una causa giudiziaria?

di Jennifer Basso Ricci

È un dato di fatto che gli strumenti tecnologici rappresentino un elemento ormai imprescindibile del vivere quotidiano, e l'informatica - unita alla telefonia mobile - sia diventata la piattaforma su cui svolgiamo la maggior parte delle nostre attività.
Non deve sorprendere allora che i dispositivi **Internet of Things** si trovino sempre più spesso in quelle che chiamiamo "le scene del crimine", diventando - a vario titolo - un vero e proprio "archivio di informazioni" per la Polizia Giudiziaria. Questo perché i device forniscono informazioni che, sotto formato digitale, riguardano dati fisici e personali - come il battito cardiaco o il numero di passi o le abitudini del sonno - e sono in grado di raccontare fatti, azioni o circostanze di interesse processuale. Oggi, poter dimostrare l'utilizzo di un determinato Pc o di un dispositivo connesso alla rete, in un luogo e ad una certa ora, e poter risalire alle precise attività svolte, può consentire di avere in mano una prova (a carico dell'accusa) o di costituirsi un alibi (a discarico).

Esempi di casi giudiziari

In molti ricorderanno il caso di **Richard Debate** (Connecticut, 2015) che venne ritenuto responsabile dell'omicidio di sua moglie grazie alla testimonianza resa dal **Fit-bit** che indossava la donna prima di morire: i dati raccolti dal "*wearable*", infatti, avevano fatto cadere fin da subito l'alibi raccontato dal marito, condannato in via definitiva a 65 anni di carcere nel maggio del 2022. Dalle informazioni ottenute dal Fit-bit, infatti, si era potuto ripercorrere tutto ciò che la signora Dabate aveva fatto nelle ore prima di essere uccisa, da quando aveva lasciato la palestra alla durata del viaggio verso casa fino all'arrivo in garage e ai suoi movimenti nelle stanze (dalla macchina al portone si dovevano percorrere non più di 125 passi - e lì, secondo la versione del marito, alle ore 9.00 del mattino, avrebbe trovato la morte per mano di un rapinatore). Il Fit-bit, invece, aveva registrato ben più di 1.200 passi e il battito della donna aveva cessato dopo le ore 10.00. In aggiunta al Fit-bit, il computer dell'uomo aveva dimostrato che lui non era in casa quella mattina – come aveva sostenuto - ma aveva mandato delle mail ai suoi dipendenti mentre era in strada. Ma ci sono altri casi giudiziari in cui è stato usato il Fit-bit. In un procedimento penale di denuncia per violenza sessuale, il Fit-bit indossato dalla vittima era riuscito a fornire la prova (a discolpa dell'imputato): la sedicente vittima, infatti, aveva dichiarato di essere stata sorpresa addormentata, mentre il suo *wearable* aveva rivelato che era sveglia e in movimento, presumibilmente ad allestire la scena di violenza. In un processo civile, instaurato dalla vittima di un incidente per la richiesta di risarcimento dei danni invece, il Fit-bit, ancora una volta indossato dalla vittima, aveva consentito di mettere a confronto le attività fisiche prima e dopo l'incidente e si è potuto appurare come

non vi fosse stata alcuna reale limitazione nelle attività. La pretesa risarcitoria era pertanto naufragata.

La prova digitale

Fatta questa premessa di contesto circa l'attualità del fenomeno IoT anche in sede processuale, passiamo adesso a trattare il tema della prova digitale per affrontare subito i suoi principali punti di debolezza della digital forensics. Partiamo da un principio giuridico basilare: la qualità principale di una prova è la sua attendibilità. Proprio su questo fronte, si evidenziano le prime - e maggiori- problematiche, collegate alla delicata fase di acquisizione e di utilizzo delle evidenze generate dai prodotti connessi alla rete o archiviate nel cloud, delle quali va garantita la massima affidabilità. Per contestualizzare e comprendere meglio il tema che stiamo trattando, si deve partire dalla nozione di *"prova"* perché, nell'ambito di ogni processo, il Giudice è tenuto a ricostruire la verità processuale sulla base delle prove che vengono dedotte nel giudizio. La funzione principale della prova possiamo dire, quindi, che sia quella di consentire al giudice di ricostruire nel modo corretto i fatti che si è riusciti a dimostrare nel corso del processo. In linea generale, non è consentito dal nostro ordinamento il ricorso a mezzi probatori non previsti o difformi dal catalogo legale: si chiama «principio di legalità». Questo principio, però, è mitigato dalla possibilità che il Giudice, quando è richiesto, possa assumere prove non disciplinate dalla legge, nel caso risultino idonee ad assicurare l'accertamento dei fatti e non pregiudichino la libertà morale della persona. Si tratta della cosiddetta *"prova atipica"*, contemplata in via generale dall'art. 189 del Codice di Procedura Penale, che richiede una condizione specifica per essere ammessa in sede processuale: *"il giudice provvede all'ammissione della prova atipica solo dopo avere sentito le parti sulle* 'modalità di assunzione' *della prova stessa"*. Me se, tradizionalmente, il metodo era basato su regole di giudizio riconosciute e accettate comunemente, come il senso comune, le conoscenze empiriche, gli strumenti culturali o le massime d'esperienza, ultimamente questo metodo "tradizionale" è entrato in crisi perché sempre più spesso i fatti rilevanti di un processo penale possono o devono essere dimostrati con teorie basate su leggi scientifiche o con procedure e strumenti tecnici. E proprio in questo contesto giuridico si colloca la prova (scientifica) atipica digitale o digital evidence.
La prova informatica possiamo dire che sia una qualunque informazione, tradotta nel linguaggio utilizzato dalle strumentazioni informatiche non immediatamente intelligibili dall'uomo, memorizzata o trasmessa in un formato digitale, che assolve alla

medesima funzione di tutte le altre prove anche se, per le sue caratteristiche intrinseche, presenta problematiche delicate e complesse. La particolare natura immateriale e volatile dei dati contenuti in un dispositivo tecnologico comporta che essi possano essere modificati, alterati, danneggiati, distrutti anche inavvertitamente, da un'errata operazione, specialmente da chi non è tecnicamente preparato a cercare, esaminare ed estrarre elementi di prova da un apparecchio digitale. Per la semplicità con cui una prova digitale può essere compromessa si rende pertanto necessario adottare cautele e procedure atte a individuare ed acquisire una prova che possa superare il giudizio di idoneità del giudice. Gli organi di Polizia Giudiziaria dovranno perciò impiegare estrema attenzione nel momento di acquisizione della prova digitale che dovrà essere estratta in maniera tecnicamente idonea, così da garantire l'inalterabilità della memoria del dispositivo. Va subito detto, però, che - dal punto di vista tecnico - esiste una numerosa serie di protocolli operativi standardizzati, riguardanti la procedura di acquisizione della prova scientifica digitale. Il problema è che questi protocolli non sono tutti omogenei, né allineati, oltre a dover essere sempre sottoposti ad aggiornamenti indotti dal rapido mutamento delle scienze e delle tecnologie.

Buone pratiche di Digital e Network Forensics

Cosa succederebbe alla prova, se dovesse emergere che la polizia giudiziaria o il pubblico ministero non avessero adottato le migliori pratiche di Digital Forensics? Sarebbe vietato al giudice utilizzare la prova per motivare la propria decisione. Tecnicamente, il giudice potrebbe dichiarare la *"nullità"* della prova oppure la sua *"inutilizzabilità"*. Ad ogni modo, la prova – proprio perché poco attendibile, non sarebbe idonea (da sola) a fondare un giudizio di colpevolezza. Quando la prova digitale non è archiviata e conservata in un hard-disk, bensì in movimento nella rete e archiviata nel cloud, come si dovrebbe procede alla sua acquisizione? Qui entra in gioco il passaggio dalla Digital Forensics alla Network Forensics, che ci aiuta a comprendere le ulteriori problematiche processuali connesse a quest'ultima frontiera della disciplina forense.

Partiamo dai fondamenti

Per Internet of Things si intende quel percorso nello sviluppo tecnologico in base al quale, attraverso la rete internet, potenzialmente ogni oggetto dell'esperienza quotidiana acquista una sua dignità nel mondo digitale. L'IoT si basa infatti sull'idea di oggetti interconnessi tra loro, integrati all'interno dell'infrastruttura internet, in modo da scambiarsi le informazioni possedute, raccolte o elaborate. Il concetto di interconnessione tra i dispositivi ha una ricaduta diretta sul tema di dove andare a cercare le prove digitali. Per questo serve conoscere la struttura del prodotto IoT: di base, il device è connesso a un router, il quale, a sua volta, è connesso a un Cloud Service Provider. I dati rilevanti possono quindi essere estratti dalle tre componenti:

1 | **da una memoria locale del device IoT (lo User Layer, cioè è la componente IoT che entra in contratto con l'utente);**
2 | **dai flussi del traffico di rete in entrata e in uscita dai gateway (la Proximity Network, cioè la rete, che connette il dispositivo IoT con il Cloud Service Provider):**
3 | **dal server in cloud (il Public Cloud, che contiene i dati dell'utente nell'ambito dell'account personale).**

In generale, una delle sfide principali nel condurre investigazioni su questi dati consiste nel preservare la catena di custodia in considerazione della volatilità dei dati (che peraltro è diversa anche a seconda della componente), posto che device/gateway/cloud continuano a comunicare attivamente tra loro. Alle citate tre componenti, corrispondono indicativamente tre aree della digital forensics. Ogni area deve essere oggetto di idonea investigazione e quindi se ne devono possedere le giuste conoscenze. C'è il "gruppo dei dispositivi IoT" (di cui al precedente numero 1) che si riferisce alle memorie locali dei device connessi alla rete. Di questi si occupa la Traditional Forensics, che, oltre ai tradizionali problemi connessi alla facile alterabilità del dato digitale, deve fare i conti con altri fattori critici contingenti, quali la varietà

della tipologia di hardware design, la differente capacità dei tool di digital forensic e, ovviamente, l'expertise dell'investigatore rispetto a quello specifico device. Poi c'è la componente della rete internet (di cui al precedente numero 2), di cui si occupa la Network Forensics, che si interessa a come avviene il traffico di rete. Infine, c'é la componente del public cloud e quindi dei dati in cloud (di cui al precedente numero 3), di cui si occupa la Cloud Forensics.

La Forensics Investigation del Cloud

Va tenuto conto che la Network Forensics e la Cloud Forensics non possono operare a *'compartimenti stagni'*, tanto che la Cloud Forensics è considerata un sottoinsieme della Network Forensics. Da sottolineare anche un altro aspetto, e cioè che la Traditional Forensics e la Network Forensics - finché quest'ultima interessa la Proximiy Network (il router) -, non richiedono, ai fini investigativi, grande collaborazione da terze parti, mentre la Forensics Investigation dei Cloud richiede allo stato (in carenza di specifici obblighi legali) la collaborazione dei Cloud Service Provider, per superare i problemi di giurisdizione. I principali Cloud Service Provider (Amazon, Google, ecc.), infatti, hanno data center in tutto il mondo e in diverse giurisdizioni. I dati memorizzati in un data center, peraltro, vengono replicati in più posizioni per garantire ridondanza e ridurre il rischio di un singolo "*point of failure*". E questi punti di replica sono potenzialmente in giurisdizioni diverse. Di conseguenza la collaborazione tra Cloud Service Provider, utente e Forze dell'Ordine è richiesta nella maggior parte dei casi di analisi legale dei Cloud.

La mancanza di standard internazionali

Inoltre, un'altra problematica legale della Cloud Forensics è data dalla carenza di standard internazionali per la Cloud Investigation, come peraltro avviene per la classica Digital Forensics. In ambito IoT, infatti, i metodi tradizionali di estrazione delle prove digitali entrano in difficoltà. Negli ultimi anni i ricercatori hanno cercato di sviluppare dei framework specifici per l'IoT così da garantire l'integrità dei dati raccolti dagli investigatori. Ad esempio, alcuni ricercatori hanno proposto un framework specifico per l'IoT, ma compatibile con gli standard Iso 270043:2015. Si tratta del *"Generic digital forensic investigation framework for IoT"* edito nel 2016. Tutta questa frammentazione tra giurisdizioni e protocolli tecnici ci porta a capire l'importanza delle prospettive internazionali, in particolari europee, in materia di cooperazione giudiziaria. In questi termini, l'adozione di una Decisione da parte del Consiglio d'Europa - lo scorso 14 febbraio 2023 - che autorizza gli Stati membri a ratificare il Secondo Protocollo addizionale alla Convenzione di Budapest (la cosiddetta *"Convenzione sul Cybercrime"*) potrebbe rappresentare un passo avanti significativo per migliorare l'accesso transfrontaliero alle prove digitali. Sulla stessa linea, il 25 gennaio 2023, Il Consiglio ha confermato l'accordo con il Parlamento europeo per l'approvazione del Regolamento e-evidence (relativo agli ordini di produzione e di conservazione di prove elettroniche in materia penale) e della Direttiva (recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali) che pone l'obbligo, per gli Internet Service Provider o i Cloud Provider, di designare un rappresentante legale nell'Unione, ai fini dell'acquisizione di prove nei procedimenti penali.
Ci si auspica, a questo punto, che il processo di definizione di un quadro normativo armonizzato, europeo e internazionale, prosegua senza interruzioni o indugi, e veda la sua tempestiva attuazione.

Una problematica legale della Cloud Forensics è data dalla carenza di standard internazionali per la Cloud Investigation, come peraltro avviene per la classica Digital Forensics. In ambito IoT, infatti, i metodi tradizionali di estrazione delle prove digitali entrano in difficoltà. Negli ultimi anni i ricercatori hanno cercato di sviluppare dei framework specifici per l'Internet of Things, così da garantire l'integrità dei dati raccolti dagli investigatori.

L'autrice

Iscritta nell'albo degli avvocati del foro di Milano dal 2006, **Jennifer Basso Ricci** ha esercitato la professione forense dal 2002 in uno studio milanese di primaria importanza in ambito penalistico. Oggi si occupa di aspetti legali connessi alla compliance aziendale, fornendo consulenza giuridica in prevalenza nel settore della responsabilità amministrativa degli enti, è Associate Partner at Partners4Innovation e membro della Community Women for Security.

Investigare senza confini

Per operare all'estero, è basilare connettersi con una rete affidabile di professionisti, che sappiano operare secondo le procedure dei rispettivi Paesi, soddisfacendo le esigenze del richiedente, seppur abituato a istituti e prassi differenti.

di Laura Giuliani

Il settore delle investigazioni private ha subito negli ultimi anni una notevole evoluzione sia sotto il profilo operativo che legislativo, a livello nazionale e internazionale. Fattori come la globalizzazione, le vicende geopolitiche, la crescente multietnicità, il passaggio all'informazione digitale, il sorgere di reati informatici o perpetrati con l'uso di sistemi digitali, hanno radicalmente modificato l'approccio professionale alle esigenze dei committenti e portato l'analisi investigativa su basi transfrontaliere. A questi grandi cambiamenti ha poi risposto il sistema giuridico, con nuove norme che hanno seguito l'evoluzione della società, del mercato e del mondo economico/finanziario, aprendo anche a nuove possibilità di azione per noi investigatori sia a livello di singole nazioni che di istituzioni internazionali. L'investigazione privata assurge dunque a un ruolo sempre più internazionale: anzitutto perché gli illeciti civili e penali assumono connotazioni transnazionali, secondariamente perché le richieste di indagine privata da e per l'estero sono sempre più frequenti, infine, perché l'operatività deve adeguarsi alla legislazione e alla giurisprudenza non solo nazionale e internazionale, ma anche di istituzioni sovranazionali. L'investigatore privato ha dovuto adeguarsi a quest'evoluzione tecnica, operativa e legislativa che si proietta necessariamente verso l'internazionalizzazione, costituita primariamente da una nuova forma mentis e da nuove conoscenze, ma anche da un buon bagaglio culturale, che non si limita alle mere conoscenze linguistiche di idiomi quali l'inglese e lo spagnolo, ma che riguarda anche la conoscenza di abitudini e mentalità differenti dalle

nostre. Dinamicità e multidisciplinarietà sono ormai elementi essenziali per svolgere questa professione che prevarica i confini dello Stato con un'accelerazione continua.

La collaborazione internazionale

Dall'analisi di questi fattori oggettivi scaturisce l'ovvia necessità di adeguare l'attività di investigatore privato al mercato internazionale. Ad esempio, in ambito privato-familiare, il numero crescente di matrimoni misti comporta la necessità dell'investigatore di essere al corrente delle soluzioni adottate in diverse giurisdizioni in relazione allo scioglimento del matrimonio, all'affidamento di figli minori o addirittura a illeciti come la sottrazione di minori. La stessa problematica, spostando l'attenzione all'ambito privato aziendale, emerge in relazione agli illeciti contrattuali, la cui prova diventa più complessa in proporzione al numero di Stati coinvolti nel contratto: ad esempio, possiamo pensare al caso di un'impresa multinazionale con sede negli Stati Uniti, la cui filiale olandese assume un procurement manager francese residente in Germania, con contratto disciplinato dalla legge inglese. Inoltre, in ambito penale si moltiplicano il numero e le modalità d'esecuzione dei reati informatici, assumendo connotazioni sempre meno tangibili e sempre più transfrontaliere. Si pensi ancora alle *"class action"*, ora consentite anche in Italia, o a nuove opportunità di lavoro, con una sempre più rilevante collaborazione con le autorità pubbliche nazionali e transnazionali; si tratta di casi di scambi commerciali, antisabotaggio e antiterrorismo, tutela del know-how, *"money laundering"* e *"whistleblowing"* (ndr: sull'argomento si veda articolo di Elisabetta Busuito nelle pagine seguenti). L'associazionismo e la costituzione di network affidabili e collaudati in cui far rientrare costanti rapporti di lavoro reciproco da/per l'Italia, facilita dunque l'attività investigativa privata.

L'attività condotta in Italia per committenti stranieri

Gli investigatori privati autorizzati hanno facoltà di esercitare l'attività sul territorio italiano indipendentemente dalla nazionalità del committente. La prassi investigativa internazionale è ormai consolidata sull'esigenza di avvalersi di professionisti locali per diversi motivi, tra cui la conoscenza della legislazione nazionale, che consente di agire in conformità all'ordinamento giuridico e alla normativa in materia investigativa, al fine di eseguire un'investigazione che fornisca elementi validi come prova in sede giudiziaria, di contenzioso o decisionale, soprattutto ai fini della protezione dei dati personali. Una delle principali difficoltà è data da alcuni istituti giuridici suscettivi di protezione, riconosciuti da un ordinamento e non da altri, soprattutto tra paesi di *"common law"* e *"civil law"*, cosicché cambia lo schema probatorio e dunque l'attività investigativa applicabile. Come spiegare a un cittadino Usa che in Italia si può provare in via documentale e testimoniale la titolarità di una *"servitù prediale"*? Oppure come far comprendere all'imprenditore italiano il concetto di *"trust"* stipulato tra *"trustee"* e *"beneficiary"*? In considerazione della conformità alla legislazione locale, assume poi rilievo la modalità di acquisizione della prova ai fini della sua utilizzabilità; infatti, in Italia alcuni dati sono pubblici, acquisibili velocemente e lecitamente e quindi assumibili come prova documentale, mentre gli stessi dati possono non essere ugualmente acquisibili in altri Stati se non commettendo un illecito. Ad esempio, la consultazione dei registri Aci-Pra per risalire al proprietario di un veicolo attraverso la targa in Italia è libera, mentre non è consentita in altri Paesi come Spagna e Francia, in quanto riservata agli organi giudiziari di polizia. Oppure, in Italia, la residenza anagrafica di una persona fisica è accessibile se motivata, mentre è vietata in altri Paesi anche agli investigatori privati. Addirittura, in alcuni Paesi l'accesso ai registri commerciali è consentito solo su richiesta motivata di un avvocato, con costi elevati e tempi lunghi. In Francia e in altri Stati i dati ufficiali di una persona giuridica sono accessibili, ma non figurano dati sull'assetto proprietario, in quanto considerati riservati. In alcuni Stati degli Usa, certi dati riguardanti i precedenti penali e le detenzioni sono accessibili via Internet previo accreditamento a un portale, mentre in Italia costituiscono un dato non acquisibile da soggetti terzi rispetto all'interessato/a. Per questo, esistono regole internazionali che facilitano i rapporti tra colleghi di tutti i Paesi, volti a escludere equivoci, fraintendimenti e facilitare i rapporti tra investigatori. È fondamentale anche conoscere la possibilità di operare come investigatori privati stranieri in Italia, poiché spesso si confonde il Diritto di stabilimento ex artt. 43-48 del Trattato CE con la libera prestazione di servizi in territorio UE. Mentre la prima è soggetta alla legge dello Stato "ospitato", l'attività esercitata in regime di libera prestazione di servizi è soggetta alle disposizioni dello stato "ospitante". In generale, quindi, la prova raccolta in Italia da un investigatore autorizzato all'estero potrebbe essere invalidata da un tribunale straniero. A tal fine vi è una specifica norma che obbliga l'investigatore straniero a operare in Italia con la propria struttura previo accertamento preventivo di due requisiti: la temporaneità dell'investigazione su suolo italiano e la specifica notifica, inoltrata preventivamente almeno dieci giorni prima dell'inizio dell'attività (temporanea), al Dipartimento di Pubblica Sicurezza

All'inizio del 2023 un investigatore privato spagnolo ha soddisfatto le aspettative del cliente connazionale procedendo con un servizio di osservazione diretta in Sardegna, durato 15 giorni, nel corso del quale ha raccolto prove eclatanti contro un cittadino italiano. L'avvocato spagnolo le ha presentate in sede processuale civile presso il tribunale competente del suo Paese, attendendo una sentenza favorevole al proprio cliente. Ebbene, le prove sono state invalidate in sede processuale per carenza della menzionata notifica al Ministero dell'Interno. Il caso ha fatto giurisprudenza perché il giudice ha dovuto - *ex lege* – annullare l'utilizzabilità di tale investigazione come prova.

del Ministero dell'Interno, circa le attività che si intendono svolgere sul territorio italiano, specificando le autorizzazioni possedute, la tipologia dei servizi, l'ambito territoriale in cui i servizi dovranno essere svolti e la durata degli stessi. Infine, un altro aspetto che avvalora l'operatività dell'investigatore privato italiano sul proprio territorio è la vastità di abitudini e regionalismi che caratterizzano il nostro Paese. Un esempio tra tutti è la disponibilità a testimoniare dei cittadini, che, secondo la diretta esperienza di molti investigatori, tende ad essere diversa anche in base all'area di provenienza dei potenziali testimoni.

L'attività condotta all'estero da investigatori italiani

La necessità di operare in un Paese di cui non si conosce a fondo l'ordinamento giuridico, ma soprattutto l'operatività consentita all'investigatore privato, può generare comportamenti illeciti o condurre all'invalidazione delle prove raccolte. Oltre a quanto già illustrato, vi sono molte differenze operative per gli investigatori privati nei diversi Stati. L'Italia è sicuramente lo Stato in cui l'investigazione privata è maggiormente regolamentata, sia per quanto riguarda il rilascio della licenza che le modalità di espletamento dell'attività, a garanzia dei diritti degli indagati, dei terzi e a tutela dei professionisti. È largamente diffusa l'idea che all'estero gli investigatori privati abbiamo maggiori opportunità, riconoscimenti e tutele, mentre è vero il contrario. La trasposizione normativa dei principi costituzionali, avvenuta in Italia con la Legge n. 63 del 2001 sul giusto processo, ha nettamente elevato il rilievo del professionista italiano rispetto a ogni collega straniero, senza considerare la severa selezione per l'accesso alla professione. Attenzione particolare va posta, quindi, quando si opera all'estero direttamente o attraverso colleghi, poiché spesso si danno per scontate procedure che invece sono suscettive di specificazioni o richieste speciali, in conformità al diritto vigente sul territorio. Un esempio pratico è l'utilizzo del Gps sui veicoli: esso è regolamentato in Italia, consentito agli investigatori privati, e non è nemmeno più necessaria la comunicazione del suo utilizzo all'Autorità Garante per la Protezione dei dati personali, mentre è vietato in altre nazioni, non solo come ipotesi di violazione della privacy, ma anche sotto il profilo penale.

- **Germania |** In Germania, per esempio, non essendovi alcuna normativa che regolamenti l'attività investigativa, l'acquisizione di prove in ambito civile, penale o in via preventiva non è sottoposta a legislazione settoriale, salvo il giudizio di ammissibilità del giudice procedente. Nemmeno è codificata l'attività più incisiva delle investigazioni difensive, da noi normata fin dal 1989, né vigono riferimenti al potere di ricerca, individuazione e acquisizione dei mezzi di prova riconosciuto al difensore dell'accusato/imputato. Nel sistema giuridico tedesco vi è sul tema una lacuna normativa: l'avvocato ha una mera funzione di impulso dell'attività istruttoria del giudice attraverso la cosiddetta *"Der Beweisantrag"*, cioè un'istanza probatoria che può essere sottoposta al giudice in ogni fase del procedimento.
- **Francia |** In Francia, gli investigatori privati possono operare previo ottenimento di una licenza, rilasciata e controllata dal **Cnaps** *(Consiglio Nazionale per le Attività di Sicurezza Privata),* sotto la giurisdizione del Ministero dell'Interno, che però non conferisce alcuno status ufficiale al titolare. La licenza, infatti, non è in alcun modo di rilievo presso le autorità pubbliche. Addirittura, su specifica richiesta del Ministero dell'Interno, nel report redatto dall'investigatore deve essere integralmente inserita una frase che attesti tale mancanza di privilegi e poteri, così come sulle perizie degli investigatori privati e addirittura sui relativi preventivi commerciali. Quindi, nonostante esista la professione di *"Private Research Agent"*, non è concesso alcun titolo ufficiale, secondo quanto stabilito da una legge statale del 1983, modificata successivamente nel 2012. Analoga carenza di poteri investigativi è presente nel processo penale, ove al difensore dell'indagato il sistema giuridico francese non riconosce particolari poteri d'indagine, poiché è al giudice istruttore che viene affidato il compito di ricercare e assumere le prove, sia quelle a carico che a discarico, sul presupposto che la tutela dell'imputato sia sufficientemente garantita dall'eser-

cizio dell'indagine pubblica. Nonostante ciò, vige in Francia il principio della libertà delle prove ex art. 427 c.p.p. francese, che consente di provare il reato con ogni mezzo di prova, da esaminarsi poi nel contraddittorio tra le parti, riconoscendo implicitamente al difensore e quindi all'investigatore privato tale facoltà d'indagine.

- **Spagna |** In Spagna, per operare in ambito investigativo privato è necessario l'ottenimento di una licenza personale (denominata Tip), rilasciata dal Ministero dell'Interno valutata la sussistenza di taluni requisiti simili a quelli richiesti dalla legge italiana. È forse lo Stato che sotto il profilo legislativo s'avvicina maggiormente al nostro nella sola fase del rilascio della licenza. Una volta ottenuta la licenza però il discorso cambia "sul campo", poiché dal punto di vista operativo l'investigatore spagnolo non gode di privilegi o riconoscimenti né in ambito civile né in quello penale. Il sistema processuale spagnolo ha subito diverse riforme, tra cui quella del 2002 che di fatto non ha ampliato i poteri del difensore e quindi dell'investigatore privato sino al punto da sancire il diritto di svolgere autonomamente indagini difensive, né lo ha reso effettivo partecipe dell'acquisizione degli elementi di prova durante la fase delle indagini preliminari. Al difensore, infatti, nella fase di prima comparizione davanti al giudice, è riconosciuta la sola possibilità di sollecitare lo svolgimento di ulteriori indagini ritenute indispensabili, ma la decisione è comunque rimessa alle valutazioni del giudice, il quale si avvale dell'esclusiva raccolta probatoria dell'Oficial, figura equivalente al nostro Pubblico Ministero, che ha pieni e unici poteri d'indagine.
- **Paesi britannici |** Un discorso a parte è riferibile ai Paesi di *"common law"*. Nel Regno Unito, gli investigatori privati non necessitano di una specifica licenza per operare sul territorio, né esiste un'autorità di controllo, salvo per quanto concerne la privacy. Per questo motivo gli investigatori privati britannici hanno adottato una sorta di autoregolamentazione e si sono dotati di un severo codice etico, che è attualmente al vaglio per essere adottato a livello europeo. Per quanto concerne gli Usa, la situazione varia da Stato a Stato, in relazione sia alla necessità di un'autorizzazione che alla regolamentazione della professione, mentre una licenza è obbligatoria per operare in tutti gli Stati dell'Australia (con esclusione dell'*Australian Capital Territory,* area di Canberra). L'evoluzione della "common law" ha prodotto per sua natura il sistema accusatorio nel processo penale e il modello di processo civile *"adversary"*. In particolare, Usa, Australia e Regno Unito, trovano nelle investigazioni difensive uno dei momenti centrali e precipui, essendo il processo basato sull'iniziativa delle parti nella ricerca, individuazione e presentazione dei mezzi di prova e sul principio della formazione delle prove in contraddittorio, in un giudizio pubblico garantito al massimo grado dalla presenza della giuria popolare. L'ampia facoltà di indagine riconosciuta alla difesa sin dall'inizio del procedimento penale assume ancor più rilevanza in questi Paesi in ragione dell'assenza di un obbligo giuridico di procedere, come invece prescritto all'art. 112 della Costituzione Italiana, sicché ricercare e acquisire elementi favorevoli all'imputato può incidere sulla stessa decisione della Procura di esercitare l'azione penale. Al contrario, una peculiarità degli Stati di common law è l'attribuzione agli investigatori di un'attività preclusa per legge ai colleghi italiani, consistente nel *"process serving"*, ossia l'attività di notificazione di atti giudiziari. Tale attività è consentita in Italia all'Ufficiale Giudiziario e, con novità introdotta dalla Legge n. 53/1994, anche agli avvocati. L'assunto trova origine da una differente formulazione degli istituti giuridici dei due ordinamenti: anzitutto, nella maggior parte dei Paesi di *"common law"*, non è previsto un sistema di localizzazione delle persone fisiche attraverso i concetti di residenza anagrafica, domicilio o dimora; inoltre in tali Stati la mobilità delle persone, che concepiscono peraltro il senso di proprietà in modo diverso dal nostro, è elevata. Ne consegue che non è applicabile la procedura secondo la quale è possibile inviare una "raccomandata" o recapitare il plico all'indirizzo ufficiale di residenza o domicilio e non è conosciuto il concetto di "giacenza" e corollari. In questo contesto è valida come prova della notifica la localizzazione del destinatario ovunque esso si trovi (anche in auto) e l'effettiva provata consegna del documento da recapitare (si veda al proposito il riquadro).

Gli strumenti di cooperazione internazionale

Due ulteriori aspetti presentano interesse d'analisi. Il primo concerne le investigazioni che hanno inizio in Italia e inaspettatamente proseguono in uno Stato estero, come il caso del pedinamento di una persona che in auto parte da Roma per andare a Milano e invece prosegue oltre frontiera su territorio francese, magari con un Gps applicato alla carrozzeria dell'auto, perché consentito dalla legge italiana. Mentre esiste una regolamentazione internazionale tra Stati confinanti per le attività espletate dagli organi giudiziari pubblici, non vi sono menzioni in relazione alle attività espletate dall'investigatore privato su incarico del cliente o difensore per il settore penale. Questo è il motivo per cui è necessario tessere una solida rete di collaborazioni tra colleghi di ogni Paese. Personalmente mi è più volte capitato di allertare un collega

straniero affinché proseguisse sul suo territorio un pedinamento iniziato in Italia. Ancora una volta emerge la necessità di conoscere la legislazione locale, poiché se il pedinamento viene proseguito e nello Stato in cui ci si trova vige una regola come quella italiana si rischia di invalidare le prove raccolte. Il secondo riguarda la mancanza di una legislazione uniforme tra Stati nelle due fasi determinati dell'attività investigativa: il rilascio di un'autorizzazione uniforme che abiliti all'espletamento della professione quantomeno in Europa, e una normativa che autorizzi il pieno espletamento dell'attività investigativa all'estero da parte degli investigatori privati autorizzati in un singolo Stato. Vi è stato in realtà un tentativo di uniformazione degli standard di accesso alla professione a livello europeo, finalizzato a individuare le peculiarità di ogni singolo Stato, garantire il soddisfacimento delle necessità di ogni Carta costituzionale e elevare gli standard di accesso alla professione. Mi riferisco allo studio condotto tra il 2004 e il 2007 dalla **Ikd** *(Internationale Kommission der Detektiv-Verbande),* la federazione europea che unisce le associazioni nazionali di categoria. La Commissione di lavoro composta dalla sottoscritta per l'Italia, dal rappresentante spagnolo e dal rappresentante dei Paesi di matrice anglo-sassone, ha sviscerato tradizioni e differenze giuridiche dei vari ordinamenti europei in materia investigativa, adattato i principi giuridici e le normative esistenti e prodotto un documento ufficiale, passato al vaglio di giudici e stampa internazionale, prima di essere presentato e approvato nell'ottobre 2007 a Zaragoza, in Spagna, e proposto a livello istituzionale europeo, nei singoli Stati prima e all'Unione Europea poi. Tale documento suggerisce un protocollo normativo per uniformare i requisiti di accesso alla professione, di mantenimento della titolarità, dell'adesione a un codice etico. In effetti, tali principi sono stati accolti in Italia nel Decreto Ministeriale n. 269 del 2010, che regolamenta a tutt'oggi l'attività investigativa nel nostro settore. Quest'ultimo aspetto è suscettivo di profonda riflessione sul piano giuridico, poiché un'uniformazione a livello europeo della normativa per il settore investigativo privato consentirebbe di attuare appieno uno dei principi fondamentali vigenti in ogni Paese e costituzionalmente garantito in Italia, ovvero il principio garantista del giusto processo di parità delle armi tra accusa e difesa, che è di fatto svilito dall'impossibilità per il difensore di esercitare in forma univoca, agevolmente e proficuamente il diritto alle investigazioni difensive oltre i confini del proprio Stato.

Di fatto si palesa la necessità di creare un rimedio per il difensore che reperisca e acquisisca una prova all'estero attraverso l'opera di un investigatore privato autorizzato, poiché lo strumento della rogatoria e dell'Oei recepito recentemente con il D.Lgs. 108/2017, si rileva spesso inadeguato a soddisfare esigenze di rapidità procedurale a causa dei vincoli formali, burocratici e pratici. È ancora evidente che l'avvocato penalista che intende reperire prove per il proprio assistito al di fuori dei confini del proprio Paese, deve dipendere dall'autorità giudiziaria estera procedente o dal Pubblico Ministero a cui indirizzare le richieste di acquisizione, sottolineando ancora una volta l'impossibilità di estendere all'estero le facoltà di utilizzo dell'investigatore privato. La soluzione, quindi, non può che essere sul piano europeo con iniziative legislative che autorizzino l'attività investigativa in tutti i Paesi e consenta appieno l'attività investigativa diretta del difensore all'estero. Questa lacuna è dovuta, a mio parere, alla volontà dei singoli Stati di riservarsi il controllo su un settore, quello investigativo privato, in grande crescita sotto il profilo della rilevanza sociale, economica e giudiziaria, temendo che l'armonizzazione dei diversi sistemi si possa trasformare in una forzata omologazione. Ma la tendenza di impedire all'avvocato di effettuare indagini dirette all'estero impedisce anche l'esercizio dell'indagato di difendersi indagando. Lo scardinamento di una visione nazionalista dell'investigazione privata non può che passare attraverso una riforma delle procedure giudiziarie e della figura del difensore, poiché la giustizia e l'equità paventate richiedono oggi un intervento legislativo uniforme, che riconosca all'indagato la possibilità di ricercare, individuare e assumere prove in via autonoma anche all'estero, come sancisce il canone di legalità processuale, enucleato all'art. 6 comma 1 della Convenzione Europea dei Diritti dell'Uomo.

Process Servers: chi sono e cosa fanno

Nei Paesi che utilizzano la *"common law"* si è sviluppata una proficua attività tra i *"process servers"*, cioè coloro che si sono specializzati nella consegna "provata" di documenti processuali, con maggioranza di investigatori privati, perché un'indagine preliminare per localizzare il destinatario, soprattutto se intenzionato a sfuggire alla consegna, è necessaria. Circola tra i detective britannici un manuale pratico, che farebbe sorridere i nostri operatori, basato sulla casistica degli ultimi decenni, ove si spiega quali procedure utilizzare in casi particolari ai fini della validità e legittimità della notificazione. Dall'impiegato facilmente reperibile alle ore 18 tutti giorni presso la propria abitazione abituale, al fuggitivo a cui la notifica è provata con il *"touch"* tecnico, al truffatore seriale che vive in posti diversi ogni giorno ed è reperibile solo per strada a bordo della lussuosa vettura di turno. In questi casi è sufficiente filmare che il detective lo pedina, lo identifica, bussa al suo finestrino lato guidatore, e lascia cadere per terra la notifica (ma solo entro un metro!). Così dai colleghi che operano nei Paesi di common law fioccano richieste a noi sconosciute di notificare documenti giudiziari, *"come order to attend court for questioning, non-molestation order, locating witnesses, service of documents at a solicitors in London (tomorrow daytime), requiring documents served in the X location on Thursday this week, service of Stat Demands on a couple in NY"*, et similia.

Tutela della privacy e controllo a distanza dei lavoratori

La disciplina che norma il controllo a distanza dei lavoratori è volta a tutelare non solo la privacy, ma anche la dignità dei lavoratori. In questo contesto, un tema che si è posto con forza nel dibattito giurisprudenziale è quello dei cosiddetti *"controlli occulti"* effettuati dal datore di lavoro all'insaputa dei dipendenti.

di Marco Martorana

La disciplina del controllo a distanza dei lavoratori è caratterizzata da una particolare complessità per via dell'interazione di due specifiche normative: quella dello Statuto dei Lavoratori e quella del Regolamento europeo 2016/679, il cosiddetto Gdpr. Vi è infatti una parziale sovrapposizione delle leggi: entrambe si applicano al controllo dei lavoratori subordinati, mentre il Gdpr si applica a tutte le persone fisiche (compresi fornitori, collaboratori esterni, clienti) i cui dati vengono trattati, ad esempio perché è installato un impianto di videosorveglianza che riprende sia i dipendenti che tutti quelli che accedono ai locali aziendali.

La norma dello Statuto dei Lavoratori

L'art. 114 del Codice Privacy (che è rimasto sostanzialmente invariato dopo l'entrata in vigore del Gdpr) sancisce che *"Resta fermo quanto disposto dall'articolo 4 della Legge 20 maggio 1970, n. 300"*. Vediamo quindi, in estrema sintesi, cosa prevede questa norma dello Statuto dei Lavoratori, rubricata *"impianti audiovisivi e altri strumenti di controllo"*. La disciplina infatti riguarda l'impiego di sistemi che diano al datore anche solo la possibilità di controllare a distanza l'attività dei lavoratori, consentito solamente in presenza di una delle tre ragioni elencate nel comma 1: esigenze organizzative e produttive, per la sicurezza del lavoro o per la tutela del patrimonio aziendale. Non solo: è prevista una procedura specifica per l'installazione degli strumenti, per cui deve essere stipulato un accordo collettivo con le rappresentanze sindacali o, in mancanza di accordo, deve essere richiesta specifica autorizzazione all'Ispettorato del lavoro. Fanno eccezione alla procedura dell'art. 4 dello Statuto dei Lavoratori i controlli sugli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e gli strumenti di registrazione degli accessi e delle presenze. L'Ispettorato Nazionale del Lavoro, con le circolari 4/2017 e 5/2018, ha chiarito che rientra nella eccezione alla disciplina dell'art. 4 ogni strumento che è indispensabile al lavoratore per eseguire la propria prestazione per cui, se ne fosse privato, sarebbe impossibilitato a svolgere le proprie mansioni.

La legittimità dei controlli occulti

Vista questa procedura così rigida e improntata alla trasparenza, volta in definitiva a tutelare non solo la privacy ma

anche la dignità dei lavoratori, un tema che si è posto con forza nel dibattito giurisprudenziale e dottrinale è quello dei cosiddetti "controlli occulti", ossia quelli effettuati dal datore di lavoro all'insaputa dei dipendenti e, quindi, senza seguire l'iter dell'art. 4. Per questo è passata alla storia la sentenza della Corte di Giustizia dell'Unione Europea nel caso Lopez Ribalda e altri c. Spagna, nella quale i giudici hanno affermato la liceità delle telecamere installate all'insaputa dei lavoratori nel caso in cui questo controllo sia preordinato a verificare eventuali atti illeciti (di cui già c'è un fondato sospetto) nei confronti del datore di lavoro. In questi casi deve essere fatto un bilanciamento di interessi per capire se effettivamente le esigenze di sicurezza dell'azienda sono tali per cui dei controlli "palesi" sarebbero controproducenti e, ad ogni modo, se sia sacrificabile la tutela della privacy dei lavoratori. Questa esigenza emerge anche dalla sentenza della Cassazione n. 6174 del 1 marzo 2019, nella quale la Corte ha affermato che i controlli occulti sono legittimi se diretti all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa ma che tuttavia, nel rispetto del principio di correttezza e buona fede, il datore di lavoro deve presentare specifici indici dell'illecito a carico dei dipendenti controllati e rendere apposita informativa privacy riportandovi la possibilità di ricorrere a forme di controllo e la descrizione delle modalità con cui lo stesso può essere condotto.

Il trattamento dei dati personali

Come anticipato, è chiaro che l'utilizzo di strumenti di controllo comporta inevitabilmente un trattamento di dati personali, per cui è necessario assicurare anche la compliance al Gdpr, a partire dai principi generali sanciti dall'art. 5 del Regolamento. Un aspetto su cui la giurisprudenza e le Autorità garanti (sia in Italia che nel resto dell'UE) hanno insistito particolarmente è l'inadeguatezza del consenso del lavoratore come base giuridica per il trattamento dei suoi dati personali nel contesto lavorativo. Infatti, in questo settore, è inevitabile che vi sia uno squilibrio di potere tra datore e dipendente, che rende quindi il consenso prestato da quest'ultimo, almeno nella maggior parte dei casi, viziato, perché non libero. Risale al 2019 una pronuncia della Cassazione (la sentenza 50919 del 17 dicembre) che esclude la rilevanza del consenso scritto dei lavoratori per il trattamento dei loro dati personali tramite l'impianto di videosorveglianza, precisando inoltre che questo non sana nemmeno il comportamento illecito del datore di lavoro che non ha seguito l'iter dell'art. 4 dello Statuto dei Lavoratori. Anche nelle Linee Guida 5/2020 sul consenso dell'*European Data Protection Board* troviamo come esempio di un caso in cui è altamente improbabile che il consenso sia libero quello in cui viene chiesto al lavoratore per l'installazione di impianti di monitoraggio. Nel caso dei "controlli occulti", a maggior ragione, è chiaro che non ci si può basare sul consenso dei lavoratori – che, anzi, renderebbe inutile il trattamento, mettendoli a conoscenza dei "sospetti" del titolare.

Il legittimo interesse del titolare

Quali sono, quindi, le basi giuridiche che possono giustificare il trattamento dei dati in questo contesto? A seconda dei casi potrebbe essere applicabile quella relativa all'esecuzione di un contratto o di misure precontrattuali con l'interessato, o vi potrebbe essere un obbligo di legge del titolare, o la necessità del trattamento per salvaguardare interessi vitali dell'interessato o di un'altra persona fisica o per l'esecuzione di un compito di interesse pubblico o connesso a pubblici poteri del titolare. È chiaro però che la condizione di liceità più frequentemente invocata sarà il legittimo interesse del titolare, che deve però sottostare a un bilanciamento con i diritti e le libertà degli interessati; bilanciamento che ritroviamo, come detto sopra, anche nel caso dei controlli occulti, come viene ben chiarito anche nella sentenza della Cassazione 25732/2021, che sottolinea che questi sono consentiti *"in presenza di un fondato sospetto circa la commissione di un illecito, purché sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali,* [...] *rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto"*. Anche l'European Data Protection Board, nelle Linee Guida 3/2019 sulla videosorveglianza, con numerosi esempi sembra porre questa base giuridica al primo posto tra quelle che abbiamo visto fino ad ora in questo contesto. Va poi prestata particolare attenzione al tema della conservazione dei dati personali: ricordiamo che l'art. 5 del Gdpr enuncia, tra i principi generali, quello della limitazione della conservazione dei dati personali a un arco di tempo non superiore a quello necessario per il conseguimento delle finalità del trattamento. Indicazioni specifiche per il caso della videosorveglianza sul luogo di lavoro le troviamo nel Provvedimento del Garante privacy dell'8 aprile 2010, dove si richiede la conservazione al massimo per 24 ore, salve particolari esigenze (ad esempio per chiusura festiva dei locali). Nonostante siano ormai passati molti anni, questa indicazione continua a essere in linea anche con gli sviluppi più recenti della normativa come, appunto, l'art. 5 del Gdpr. Infine, è importante sottolineare che la violazione della disciplina sulla videosorveglianza, come affermato dal Garante privacy nell'Ordinanza ingiunzione del 1° dicembre 2022 [9838992], non può essere considerata una violazione "minore", a prescindere dal numero di dipendenti controllati: il fatto che questo sia esiguo al massimo potrà incidere sul quantum della sanzione.

Come viene chiarito anche nella sentenza della Cassazione 25732 del 2021, i controlli occulti sono consentiti *"in presenza di un fondato sospetto circa la commissione di un illecito, purché sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto".*

Chi è Marco Martorana

Avvocato presso il Foro di Lucca, Professore a contratto di Diritto della Privacy presso **Universitas Mercatorum**, Presidente dell'associazione Assodata e Data Protection Officer, **Marco Martorana** è esperto di diritto della privacy e delle nuove tecnologie. Ha partecipato come relatore a numerosi seminari ed eventi e ha pubblicato articoli, saggi e monografie sul tema. Da anni collabora con Federpol nell'attività di formazione, con particolare riferimento alle regole deontologiche nelle investigazioni difensive.

Dati personali: come, quando e dove conservarli

Alcuni elementi utili a definire i limiti e gli accorgimenti, legati alla conservazione dei dati personali, che possono aiutare gli investigatori a operare secondo scelte consapevoli e con la minore esposizione ai rischi che possono scaturire da una normativa ancora in evoluzione.

di Riccardo Martina

Il tema della conservazione dei dati è uno dei più dibattuti nell'ambito investigativo e richiederebbe ben più ampio spazio per una sua trattazione esaustiva. Il testo dell'art. 10 delle *"Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria"* in allegato 2 al D.Lgs. 196 del 2003, non lascerebbe molto spazio all'investigatore sancendo che:
«...i dati personali trattati dall'investigatore privato possono essere conservati per un periodo non superiore a quello strettamente necessario per eseguire l'incarico ricevuto... omissis... Una volta conclusa la specifica attività investigativa, il tratta-

mento deve cessare in ogni sua forma…». Unica apertura è quella offerta da una frase del comma 2 che, a mio parere, non è molto sostenibile rispetto al dettato del Reg. UE 2016/679 quando interpretata così da attribuire al *"difensore o al soggetto che ha conferito l'incarico"* il potere di autorizzare la conservazione di dati personali relativi a soggetti terzi. D'altro canto, l'investigatore deve far fronte anche ad altre esigenze di conservazione spesso irrinunciabili, volte essenzialmente a tutelare un proprio diritto e/o dimostrare la liceità del proprio operato, soprattutto nei casi evidentemente critici e sicuramente forieri di problemi futuri.

Una normativa in evoluzione

Per valutare il bilanciamento tra esigenze dell'investigatore, tutela degli interessati e obblighi è necessario evidenziare alcuni elementi utili a definire i limiti e gli accorgimenti che possono aiutare a operare secondo scelte consapevoli e con la minore esposizione ai rischi che possono scaturire da una normativa ancora in evoluzione.
In primis, la normativa in tema di tutela dei dati personali non proibisce la conservazione a condizione che la stessa:

1 | sia effettuata per una finalità legittima che si possa inquadrare in una delle basi giuridiche previste al comma dell'art. 6 Regolamento UE 2016/679 e/o al comma 2 art. 9 se la conservazione riguarda anche dati appartenenti alle categorie particolari elencate al comma 1 sempre dell'art. 9;

2 | siano rispettati tutti gli obblighi imposti dalla normativa, tra i quali assumono rilevanza le misure di sicurezza e la probabilità di dover:
- erogare una informativa ex art. 14 relativamente ai dati acquisiti da soggetti terzi e riguardanti gli interessati, che in questo caso possono essere i soggetti investigati, a meno che non si verifichi una delle condizioni previste al comma 5 dello stesso articolo;
- soddisfare le richieste di accesso ai dati (o gli altri diritti) avanzate dagli interessati ove non si verifichino condizioni previste all'art. 2-undecies D.Lgs. 196/2003.

Cito questi obblighi poiché sono "difficilmente gestibili" in tutti quei contesti in cui sia problematico procedere con azioni che vanno a palesare o confermare all'interessato l'esistenza di una attività di investigazione effettuata sul suo conto, anche se conclusa. Si pensi, ad esempio, a una attività di indagine per sospetta infedeltà coniugale o per sospetta infedeltà del dipendente, soprattutto quando queste diano un esito negativo (il sospetto era infondato).

La conservazione del rapporto e dei dati acquisiti

Come citato, la normativa non proibisce in assoluto la conservazione dei dati acquisiti: l'investigatore potrà decidere se vi siano i presupposti per giustificarne la conservazione in relazione a una attività investigativa, tenendo presente e contestualizzando i limiti imposti dal citato art. 10 delle Regole Deontologiche. L'investigatore dovrà, quindi, effettuare attente e sostenibili valutazioni circa eventuali esigenze di ulteriore conservazione dei dati derivanti ad esempio:

- **da particolari criticità rilevate durante le attività o nei rapporti con il mandante;**
- **da incongruenze rilevate rispetto alle dichiarazioni del mandante;**
- **da un effettivo e concreto rischio di contestazione.**

È opportuno che tale valutazione sia effettuata per ogni singolo caso, in modo da poter dimostrare il rispetto dei principi previsti all'art. 5 del Reg. UE 2016/679 e l'effettiva applicabilità delle basi giuridiche invocate dall'investigatore a giustificazione della conservazione di ciascun atto; ciascuna valutazione dovrà preventivamente stabilire anche un tempo massimo di conservazione di ciascun atto, poiché non esiste una "regola assoluta" valida per tutte le circostanze. L'investigatore dovrà quindi essere in grado di rispondere correttamente a questi due quesiti per ogni documento che decide di conservare:

1 | *"La finalità della conservazione è legittima e fondata su una delle basi giu-*

L'autore

Già ufficiale dei Carabinieri, dal 1991 **Riccardo Martina** si occupa di security e sicurezza militare e dal 1997 di privacy. Titolare della C.S.I. S.r.l., consulente e collaboratore di gruppi, enti, aziende e associazioni, dove ricopre il ruolo di security manager o Data Protection Officer. Partecipa a seminari e conferenze come relatore ed è docente in materia di protezione dei dati personali, risk management, security aziendale. Collabora con Federpol dal 2011.

ridiche riconosciute agli art. 6 e 9 del Reg. UE 2016/679?".

2 | *"Sono stati informati gli interessati come previsto dall'art. 14 del Regolamento UE 2016/679?"* oppure *"Per quale motivo non sono stati informati gli interessati?"*, potendo a tal proposito citare una delle esimenti previste al comma 5 del citato art. 14 o, in alcuni casi, il segreto professionale, anche allegando agli atti conservati una relazione contenente le valutazioni effettuate, in quanto potrebbe trovarsi a dover fornire una risposta sostenibile in uno dei seguenti casi:

- **Attività ispettiva da parte delle autorità competenti;**
- **Richiesta esercizio diritti ex art. 15 - anche inoltrata in modo strumentale da parte di chi sospetti o sia già a conoscenza delle attività svolte;**
- **Data breach da segnalare obbligatoriamente all'autorità Garante e, in alcuni casi, agli interessati stessi (artt. 33 e 34 del Regolamento UE 2016/679).**

In riferimento al primo quesito, nel contesto in esame, le basi giuridiche invocabili sono per la maggior marte dei casi:

- un legittimo interesse (art. 6 c. 1 lett. f) costituito dalla necessità di dimostrare la liceità del proprio operato, che, si ricorda, non trova applicazione in riferimento alle categorie particolari di dati (gli ex dati personali sensibili);
- la tutela di un diritto in sede giudiziaria, difficilmente applicabile generalmente a tutti i casi. Inoltre, si deve ricordare quando sancito dal già citato art. 10 delle regole deontologiche: *"La sola pendenza del procedimento al quale l'investigazione è collegata, ovvero il passaggio ad altre fasi di giudizio in attesa della formazione del giudicato, non costituiscono, di per se stessi, una giustificazione valida per la conservazione dei dati"*.

Per il secondo quesito il tema assume una maggiore complessità, stante il fatto che l'art. 14 non è stato, sicuramente, formulato pensando anche allo specifico contesto degli investigatori, consentendo di omettere l'informativa esclusivamente quando l'adempimento:

- risulta *"impossibile"* o implica uno *"sforzo sproporzionato e difficilmente applicabile"*;
- *"rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento"*;
- *"qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale"*, non sempre invocabile dall'investigatore.

La conservazione del mandato

Il mandato è il contratto stipulato tra l'investigatore e il mandante e, per tale motivo, deve essere conservato per 5 anni se prendiamo come riferimento la normativa fiscale, per 10 anni considerando gli artt. 2220 e 2946 c.c.. Da tenere presente che il mandato contiene tutte le informazioni sul soggetto investigato fornite all'investigatore per circostanziare l'attività richiesta.

La modalità di conservazione dei dati

In caso di ulteriore conservazione, assumono particolare importanza le misure adottate per garantire la sicurezza dei dati, che dovranno essere tali da:

- garantire che l'accesso ai dati sia consentito solamente in caso di esigenza al titolare ed a soggetti da questi specificatamente incaricati caso per caso,
- garantire nel modo più assoluto la riservatezza dei dati,
- garantire il rispetto dei tempi di conservazione stabiliti dal titolare per ogni singolo caso, ricorrendo anche:
  - per la conservazione di documentazione cartacea, ad arredi di adeguata resistenza fisica dotati di sistemi di chiusura preferibilmente elettronici in grado di monitorare gli accessi agli atti;
  - per i sistemi informatici, ad algoritmi di cifratura di adeguata robustezza, autenticazione a doppio fattore e, possibilmente, audit log, considerando che il ricorso alla cifratura riduce in modo esponenziale il rischio di dover procedere con le segnalazioni in caso di *"data breach"*.

“Pretext Inquiries”, uno strumento di indagine discusso

Le investigazioni private tra limiti normativi, esigenze investigative e “Pretext Inquiries”. A confronto la normativa negli Stati Uniti e in alcuni Paesi europei.

di Fabrizio Farris

Lo scopo dell’elaborato dal titolo **“***Le investigazioni private tra limiti normativi, esigenze investigative e Pretext Inquiries”,* con cui sono stato premiato al 66° Congresso Nazionale di **Federpol** di Giardini Naxos in Sicilia, è stato quello di spiegare a fondo l’investigazione privata partendo dalle sue origini nella Francia ottocentesca con Eugène-François Vidocq, passando per Chicago con Allan J. Pinkerton, e la sua agenzia investigativa privata più famosa al mondo, la Pinkerton National Detective Agency. Nel nostro Paese la diffusione delle investigazioni private fu molto più lenta e solo con il Regio n. 773/1931, venne approvato il Testo Unico delle Leggi di Pubblica Sicurezza in cui vennero elencati alcuni presupposti per l’attività investigativa subordinata al rilascio di licenza prefettizia ex art. 134 Tulps, regolando così gli Istituti di Investigazioni private e di Informazioni commerciali. Tale normativa è rimasta immutata fino a quando fu emanato, a seguito di un lungo iter monitorato dalla Federpol, il Decreto del Ministero degli Interni n. 269/2010, che ha riformato il mondo delle investigazioni private sia da un punto di vista giuridico che tecnico-operativo.

L’investigatore e la tutela della privacy

Un tema molto importante che ha richiesto e richiede maggiore attenzione è quello relativo alla tutela della privacy. All’interno della Comunità Europea le direttive 95/46/CE e 97/66/CE ribadirono il concetto della tutela della riservatezza dei dati personali. In Italia, la prima di queste, venne recepita con la Legge n. 675/1996 ma il suo iter fu molto complesso in quanto il Ddl penalizzava fortemente

gli investigatori privati, perché li obbligava a informare la persona sottoposta a indagine e a chiedere il consenso prima ancora dell'inizio delle indagini. L'assurdità spinse centinaia di investigatori privati a manifestare a Roma il disagio e le preoccupazioni della categoria portando alla revoca dell'obbligo di avvisare preventivamente l'indagato. Con l'approvazione di questa venne introdotto il concetto di Privacy fino alla definitiva approvazione nel 2003 del cosiddetto *"Codice della Privacy"*. Nel 2016 Parlamento e Consiglio europeo hanno emanato il nuovo Regolamento 2016/679 che prevede delle regole che debbano essere obbligatoriamente rispettate, abrogando la precedente Direttiva 95/46/CE. Tale documento viene identificato come Gdpr *(General Data Protection Regulation),* strumento essenziale per garantire la protezione dei dati personali degli individui nell'era digitale. Grazie a questa importante normativa sono stati rafforzati i diritti dell'interessato, che sarà a conoscenza dell'uso dei suoi dati, permettendo però la libera circolazione degli stessi.
La parte centrale dell'elaborato è dedicata all'equilibrio tra la tutela della privacy e l'esigenza investigativa in quanto l'investigatore privato resta ancora penalizzato rispetto alla categoria del giornalista investigativo, del privato cittadino e dei "mistery shopper". A titolo di esempio, il Codice deontologico relativo al trattamento dei dati personali nell'attività giornalistica, spiega che il giornalista deve rendere note le proprie generalità e le finalità di raccolta, salvo che questo comporti rischi per la sua incolumità quando raccoglie ogni notizia utile mentre, le regole deontologiche, obbligano l'investigatore privato a fornire l'informativa agli interessati nei casi in cui vi sia interazione diretta. L'attività del giornalista investigativo però è diretta alla "divulgazione" delle informazioni acquisite, che potrebbe comportare una operazione potenzialmente lesiva per la tutela degli interessati, mentre l'attività dell'investigatore è quella di "comunicare" i propri risultati solamente al proprio committente. Alla luce di ciò vi è un'evidente e ingiustificata disparità di trattamento; infatti, l'attività investigativa privata dovrebbe beneficiare della stessa esimente prevista per la professione giornalistica, in special modo quando opera in contesti particolarmente pericolosi come quello, ad esempio, della criminalità organizzata.

Pretexting Inquiries e normativa

Per concludere è stato doveroso focalizzare l'attenzione anche sulle *"Pretext Inquiries",* uno strumento di indagine utilizzato per raccogliere informazioni difficili o impossibili da ottenere se l'investigatore rivelasse la propria qualifica o la motivazione dell'indagine. Ad esempio, l'investigatore privato per ottenere le informazioni desiderate potrebbe fingersi un rappresentante di un'azienda, oppure un cliente interessato a servizi o prodotti. Si è condotto uno studio sugli Stati Uniti e su diversi Paesi europei, da cui emergono

"Sono orgoglioso di questo riconoscimento. I ringraziamenti vanno al mio relatore, il professor **Alberto Paoletti**, per avermi guidato nella stesura dell'elaborato, al presidente di Federpol **Luciano Tommaso Ponzi** e al master da me frequentato. Impegno, passione e perseveranza mi hanno permesso di ricevere questo prestigioso premio di cui vado veramente fiero".

diverse situazioni. Negli Usa, la Federal Trade Commission definisce il *"Pretexting"* come una pratica utile a ottenere dati personali, fingendosi un'altra persona. Alcuni tipi di pretesti vengono, però, puniti dalla legge. Ad esempio, ottenere o vendere tabulati telefonici attraverso pretesti è stato reso un reato federale. Molte tecniche utilizzate da questi non sono completamente illegali, infatti creare un falso profilo social per investigare su di un soggetto non è illegale, ma viola solamente i termini di servizio. Per **Mark Halligan**, avvocato di Chicago, *"Pretexting"* significa rappresentarsi in modo tale da far ammettere a un sospettato determinate dichiarazioni che non avrebbe detto se l'investigatore si fosse presentato come tale. In particolare, la pratica del pretesto è riconosciuta quale strumento investigativo non solo per le forze di pubblica sicurezza, ma anche per gli investigatori privati autorizzati. Questi ultimi, però, sono preoccupati che la legislazione "Anti-Pretexting" possa indurre il Congresso americano a vietare l'utilizzo di uno strumento fondamentale per l'attività investigativa, con la conseguente messa al bando delle attività sotto copertura degli investigatori. La precedente legge anti-pretesto non vietava il pretesto utilizzato nelle indagini legittime, mentre la nuova legislazione pretende che le indagini vengano svolte sotto la supervisione legale al fine di valutare a fondo le conseguenze legali delle azioni e proteggere i propri interessi; infatti, al centro di molte indagini vi è la necessità di ottenere informazioni personali e molti professionisti violano la legge anche inconsapevolmente. In Germania, il Pretext degli investigatori privati è legalmente accettato nei tribunali solo a determinate condizioni. L'art. 42 della legge federale sulla protezione dei dati punisce chiunque abbia ottenuto e trattato dati personali senza averne diritto o li abbia ottenuti con un pretesto. Ma quindi gli investigatori privati hanno il diritto di ottenere informazioni personali? La legge tedesca non tratta direttamente tale questione, né esiste una licenza. Nonostante ciò, gli investigatori privati tedeschi collaborano con la polizia e sono accettati nei tribunali.

In Spagna, la normativa sulle investigazioni private, afferma che gli investigatori privati possono informare solamente il cliente e le autorità di polizia e giudiziarie in ordine alle loro richieste. Prima dell'entrata in vigore del Gdpr, il regolamento spagnolo sulla protezione dei dati spiegava che il consenso dell'interessato è richiesto *"salvo diversa disposizione di legge"*. Successivamente l'autorità spagnola per la protezione dei dati ha stabilito che gli investigatori privati sono autorizzati dalla legge a trattare i dati personali, non richiedendo più il consenso del soggetto.

Pretext Inquiries e rispetto della privacy

Quindi, l'utilizzo delle "Pretext Inquiries", nel rispetto della privacy del soggetto indagato, permette di raccogliere informazioni importanti per la ricerca della verità, il contrasto delle truffe e l'attività criminale in genere. L'auspicio è quello di arrivare a una chiarificazione da parte delle autorità competenti, al fine di non vedersi rifiutare tutte quelle informazioni raccolte attraverso questo formidabile strumento, che difficilmente sarebbero state ottenute fornendo la propria identità di investigatore privato e la finalità dell'indagine. Tale lavoro è stato reso possibile grazie al supporto del mio relatore, il professor **Alberto Paoletti**, a cui va la mia stima e il ringraziamento per il materiale fornitomi, le conoscenze trasmesse e l'intenso lavoro svolto insieme per circa cinque mesi. Inoltre, mi sento di ringraziare anche il professor **Natale Fusaro,** responsabile della segreteria didattico-scientifica del Master e docente di Criminologia e Criminalistica, per le conoscenze trasmessemi; il professor **Pierpaolo De Pasquale**, per la sua immensa disponibilità e il presidente di Federpol **Luciano Tommaso Ponzi** per avermi assegnato il premio in occasione del 66° Congresso Nazionale della Federazione che si è tenuto lo scorso maggio a Giardini Naxos in Sicilia.

Chi è Fabrizio Farris

Fabrizio Farris nasce a Viterbo nel 1996. Nel 2018 consegue la laurea in Scienze politiche e delle relazioni internazionali - Curriculum investigazioni e sicurezza all'università della Tuscia, con una tesi dal titolo *"Investigazioni scientifiche e accertamento identità"*. Nel 2019 consegue il master di primo livello in Scienze forensi e criminologiche sempre all'Unitus con una tesi dal titolo *"Caratteristiche del Fentanyl e sua diffusione nel mercato delle sostanze stupefacenti. La repressione penale alla luce delle recenti modifiche del Dpr 309/90"*. Nel 2022 consegue la Laurea magistrale in Scienze della politica, della sicurezza internazionale e della comunicazione pubblica, curriculum Investigazioni e sicurezza con una tesi dal titolo *"Prevenzione e contrasto al riciclaggio nel settore dei giochi e delle scommesse"*. Subito dopo consegue il master di secondo livello in Scienze forensi all'università La Sapienza di Roma con una tesi dal titolo *"Le investigazioni private tra limiti normativi, esigenze investigative e Pretext Inquiries"*. Con questo elaborato, in occasione del 66° Congresso Nazionale di **Federpol**, vince il primo premio al Concorso per le migliori tesi nell'ambito delle investigazioni private.

In cerca di un bilanciamento dei diritti

L'attività investigativa tra diritto alla protezione dei dati personali e libertà di impresa.

di Vincenzo Ricciuto

L'attività investigativa svolta dagli investigatori privati ha una funzione indefettibile e propria di questa attività: vale a dire che le indagini dell'investigatore privato (nella prospettiva regolatoria del diritto) costituiscono strumenti che consentono, ad altri soggetti, di difendere i propri diritti e le proprie libertà. Tale funzione dell'attività investigativa si svolge raccogliendo tutte quelle informazioni che sono necessarie per poter tutelare diritti e libertà, per poterne conoscere e percepire una eventuale lesione, per poterne dimostrare al giudice la compromissione. L'attività investigativa è in sintesi un'attività che in considerazione nella prospettiva giuridica può essere considerata quale strumento di garanzia e realizzazione di diritti e di interessi dei soggetti dell'ordinamento. E ciò, se è notoriamente percepibile nel settore penale (dove è particolarmente avvertita l'esigenza di ricercare prove per dimostrare una realtà alternativa a quella di una possibile accusa) è ancor più significativo nel nostro modello processuale civile. Il principio dispositivo e l'impossibilità per il giudice civile di cercare direttamente la prova dei fatti affermati nel processo e in definitiva l'impossibilità per il giudice di ricostruire come i fatti sono realmente accaduti, rendono indispensabile dotare i soggetti privati degli strumenti in grado di consentire loro

di recuperare prove, genuine e integre, a supporto dei fatti su cui fondano la propria domanda di tutela giudiziale o, ancor prima della prospettiva processuale, per poter valutare l'eventuale presenza di un pregiudizio o rischio per i propri diritti. Tra quegli strumenti, appunto, dobbiamo annoverare le indagini svolte dai soggetti autorizzati e dirette a raccogliere prove e in genere informazioni di cui, è solo il caso di sottolinearlo, occorre garantire integrità, genuinità, autenticità. Va da sé che la disciplina dell'attività investigativa e le regole di quella professione incidono sull'ampiezza degli strumenti di tutela che l'ordinamento pone a disposizione dei soggetti a garanzia dei loro diritti e dei loro interessi: maggiori limiti, condizionamenti e divieti allo svolgimento di un'attività investigativa incidono, ovviamente, sul ventaglio di informazioni e di prove che possono essere legittimamente raccolte e utilizzate dalle persone per esercitare e difendere i propri diritti. Le mie riflessioni guardano, dunque, a come la disciplina dell'attività investigativa quale trattamento dei dati personali incida sul fine di quell'attività, vale a dire sulla possibilità di raccolta di informazioni e prove genuine, integre, ecc.

Una regola molto generale

Il punto di riferimento normativo è, ovviamente, il Gdpr, il Regolamento Generale UE 679 del 2016. Si tratta di una disciplina molto generale, in grado di accogliere al suo interno e regolare in maniera orizzontale attività estremamente diverse tra loro e che hanno come tratto comune quello di trattare dati personali (dall'attività giornalistica, di marketing, del medico, dell'avvocato, dell'attività degli investigatori privati ecc.). La generalità della regola, tuttavia, quando così marcata, non sempre risponde alle effettive esigenze di disciplina di un fenomeno e rischia, se non adeguatamente governata attraverso un'adeguata attività di adattamento della regola generale alle specifiche esigenze del contesto nel quale essa andrà a operare, di rendere quella regola ingiusta e addirittura dannosa per i soggetti e per il sistema ordinamentale.

Se si guarda alla disciplina generale e poi a quella speciale attualmente operante per le investigazioni dettata in materia di trasparenza, è facile notare, ad esempio, lo scarso adattamento della regolamentazione speciale (per il momento contenuta in vecchie regole deontologiche che attendono opportuna e razionale riforma) alle peculiarità del settore e proprie dell'attività e della funzione svolta dall'investigatore. Il principio di trasparenza (che impone a chi tratta il dato personale di rendere, sempre, ogni aspetto di quel trattamento evidente e conosciuto alla persona dell'interessato). In via generale, dunque, qualora il dato sia raccolto presso l'interessato, il Gdpr impone di rendergli, immediatamente, totalmente trasparente l'operazione della sua raccolta e trattamento. Quando un dato debba intendersi *"raccolto presso l'interessato"* (e quindi quando bisogna avvisare subito l'interessato che si sta avviando un'operazione di raccolta e trattamento di informazioni che lo riguardano), ce lo dicono le linee guida ex art. 29 (valutazioni, in verità, che si muovono anch'esse su un piano ancora molto generale): il dato è *"raccolto presso l'interessato"* nel caso in cui egli stesso lo fornisca consapevolmente al titolare (ad esempio durante un'intervista).

L'impatto sull'attività investigativa

Traduciamo dunque quella regola generale in tema di trasparenza nel settore specifico dell'attività dell'investigatore e valutiamo la portata (o il suo "impatto") sulla realtà ed efficacia dell'investigazione, con riferimento alla cosiddetta valutazione d'impatto della regolazione. Poniamo il classico caso in cui l'investigatore, incaricato nell'ambito di un'indagine nel caso dell'intervista in cui il soggetto indagato sia contestualmente avvisato del fatto che le informazioni che darà sono necessarie per tutelare gli interessi di un'altra determinata persona anche, in ipotesi, in un potenziale contenzioso con l'indagato. Conscio del fine per il quale saranno utilizzate le informazioni che verranno rilasciate a colui che ha svelato essere un investigatore che agisce per

L'articolo n. 4 del Gdpr prevede che *"il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo…"*.

conto di un determinato soggetto, l'interessato o investigato fornirà versioni dei fatti e informazioni parziali, a sé favorevoli, se non addirittura alterate o false.

Il sacrificio di altri diritti fondamentali

Gli esempi potrebbero continuare, e arrivare anche a sfociare in possibili lesioni di diritti fondamentali della persona, compresa l'incolumità dell'investigatore stesso o del suo cliente dinnanzi al soggetto interessato al quale viene svelato, ex abrupto e in un contesto particolarmente delicato, che si intende raccogliere informazioni che lo riguardano per fini che potrebbero vederlo parte in causa, soggetto di denunce, destinatario di decisioni sfavorevoli, ecc. Al di là dei numerosi esempi possibili, ciò che emerge è una consapevolezza: il trattamento dei dati personali che costituisca esercizio di investigazione privata, in quanto attività funzionale a consentire la tutela e la garanzia di interessi e di diritti dei soggetti nell'ordinamento, necessita di una disciplina che, quanto al trattamento, tenga conto delle peculiarità del settore, dell'attività e dei suoi fini. In altri termini, ci si deve interrogare se l'applicazione acritica della normativa generale del Gdpr all'attività e al settore delle investigazioni private non vada, in realtà (e per un mero ossequio a una eccessivamente astratta idea di trasparenza a beneficio del diritto alla protezione dei dati personali dell'interessato), a sacrificare altri diritti fondamentali, altrettanto rilevanti per l'ordinamento:

- **il diritto del cliente che si intende tutelare attraverso l'attività di indagine** (che sia esso il diritto all'integrità del patrimonio aziendale o diritto di altra specie);
- **il diritto alla protezione dei dati personali del cliente** (dati che, nell'impianto dell'informativa dell'art. 13 del Gdpr, dovrebbero essere comunicati all'indagato visto che lo si deve informare dell'identità del titolare del trattamento e di coloro ai quali i dati verranno comunicati);
- **il diritto dell'investigatore di svolgere la propria attività, e a svolgerla in modo efficace e funzionale allo scopo** (diritto che, non dobbiamo dimenticare, non è solo riconosciuto dalla legislazione ordinaria che regolamenta la professione, ma è costituzionalmente tutelato come libertà d'impresa dall'art. 41 della Costituzione).

E mi pare che a questa domanda non si possa, allo stato dell'arte, che rispondere affermativamente. Una acritica trasposizione delle prescrizioni di cui all'articolo 13 in materia di informativa all'interessato e trasparenza, che non ammetta eccezioni all'obbligo di svelargli immediatamente l'indagine, il suo committente e il contenuto, non solo pregiudica i diritti del cliente e dell'investigatore, ma depotenzia uno strumento giuridico fondamentale che l'ordinamento ha voluto offrire ai privati per tutelare i propri diritti: la possibilità del ricorso alle investigazioni private. L'impressione è che si sia finiti per limitare (o vietare) alcune forme di esercizio di un'attività professionale (quella dell'investigatore), ridefinendone i confini di liceità per l'ordinamento, e per limitare altresì il diritto di difesa. E acritica appare anche la

trasposizione di quella norma generale dell'art. 13 del Gdpr nelle regole deontologiche che ancora sono vigenti per questo settore, che si limitano a riprodurre pedissequamente l'obbligo di informativa richiesto dal Gdpr, allontanandosi da quella che è la reale missione e funzione delle regole deontologiche (oggi assolta dai Codici di Condotta), che non è certo quella di riprodurre la regola generale, ma di adattarla al contesto e alle singole specificità ed esigenze del settore. L'auspicio è dunque che si torni su questa materia, in modo da offrire alla disciplina dell'attività investigativa una dimensione tale da tutelare e bilanciare non solo la protezione dei dati personali dell'indagato, ma anche gli altri diritti e libertà fondamentali che in una vicenda di investigazione sono implicati: non ultima quella della stessa impresa di investigazione. E direi che questo non è solo un auspicio, ma è proprio una prescrizione del legislatore europeo, che chiaramente invita a superare l'idea di una disciplina della protezione dei dati personali tirannica, in cui il diritto dell'interessato prevale aprioristicamente su qualsivoglia altro diritto o libertà.

Alcuni suggerimenti

Quanto allo strumento giuridico con cui questo adattamento della regola generale al settore specifico andrebbe realizzato, il riferimento è ovviamente all'adozione di codici di condotta i quali, se non vogliono incappare nuovamente nel difetto originario delle vecchie regole deontologiche, dovrebbero evitare di riportare pedissequamente il dettato del Gdpr, ma, al contrario, dovrebbero prevederne una specificità, muoversi nel solco del bilanciamento tra i vari diritti e libertà implicati, quanto, ad esempio, alla regola concreta per il settore. Alcuni suggerimenti potrebbero essere quelli volti a restringere il concetto, in questo campo, di dati "raccolti presso l'interessato" di cui all'articolo 13, con l'effetto conseguente di ampliare l'ambito applicativo dell'altro articolo del regolamento generale dedicato all'informativa all'interessato, vale a dire l'articolo 14. Quest'ultimo disciplina l'informativa dei dati raccolti *"non presso l'interessato"*, prevedendo eccezioni all'obbligo di fornire l'informativa (le quali, viceversa, non sono testualmente previste nell'art. 13): l'obbligo di informativa ex art. 14 non opera se dare l'informativa *"risulta impossibile o implicherebbe uno sforzo sproporzionato"* oppure se renderebbe impossibile o pregiudicherebbe gravemente il conseguimento delle finalità del trattamento. D'altra parte, lo stesso non distingue (diversamente dalla parte dispositiva di cui agli articoli 13 e 14) le esenzioni all'obbligo di informativa a seconda di come i dati sono raccolti. Esso si limita infatti a stabilire che *"non è necessario imporre l'obbligo di fornire l'informazione se l'interessato dispone già dell'informazione, se la registrazione e la comunicazione dei dati personali sono previste per legge o informare l'interessato si rivela impossibile o richiederebbe un rapporto sproporzionato"*.

Le potenzialità del Gdpr

I tempi sono, infine, anche culturalmente maturi per trarre tutte le potenzialità del Gdpr in ordine alla disciplina dei fenomeni, che non sono da intendere come pericolosi per i diritti della persona, ma anche come fenomeni di impresa da regolare nel bilanciamento dei diritti. Quella in tema di trattamento di dati personali è una normativa che non ha l'obiettivo di vietare attività d'impresa che abbiano ad oggetto il trattamento di dati personali (qual è tipicamente quella investigativa), ma al contrario si propone di agevolarne lo svolgimento nel suo bilanciamento con i diritti della persona.
Non può più trascurarsi, in definitiva, che il Gdpr non si limita solo a tutelare i diritti delle persone, ma si propone di realizzare la libera circolazione regolata dei dati personali, considerata benefica per lo sviluppo della società (art. 1). Sicché, in un dato contesto, come quello in esame, in cui accanto alle esigenze di tutela degli interessi dell'investigato/interessato si pongono quelle, parimenti di rilevanza costituzionale, di tutela del diritto di difesa del cliente/indagato (o convenuto, o danneggiato, ecc.) e altresì quelle *"di impresa"* dell'investigatore, occorre indubbiamente procedere senza eccessivi formalismi a un più proporzionato bilanciamento dei diritti.

L'autore

Nato nel 1959 a Duronia (CB), **Vincenzo Ricciuto** è professore ordinario di Diritto Civile nell'Università degli Studi di Roma Tor Vergata, dal 2006. Ha svolto attività di ricerca presso la Columbia University di New York e presso l'Universidad de Barcelona. È autore di volumi monografici sul contratto; saggi e articoli sulle tematiche classiche del diritto civile, pubblicati sulle principali riviste giuridiche, coautore e curatore di volumi sul diritto dell'economia e sul diritto delle nuove tecnologie e coautore di un Manuale di Diritto privato.

Come investigare sul dipendente infedele

È possibile prevenire e individuare eventuali tentativi di furto o diffusione impropria dei dati aziendali da parte dei dipendenti, attraverso l'utilizzo di strumenti tecnologici avanzati e rivolgendosi al supporto delle competenze di un investigatore privato.

di Fabio Di Venosa

La crescente diffusione delle tecnologie digitali e l'accesso sempre più semplice alle informazioni aziendali hanno aumentato il rischio che i dati aziendali possano essere oggetto di furto o di diffusione impropria da parte dei dipendenti, che rappresentano il primo anello della catena di sicurezza dell'azienda. È possibile però mettere in atto misure di

prevenzione efficaci per evitare che il dipendente possa diventare un rischio per l'azienda.

Il ricorso all'investigatore privato

Fermo restando i limiti normativi dettati dallo Statuto dei lavoratori sul controllo dei dipendenti, è infatti legittimo demandare a un'agenzia investigativa munita di regolare licenza prefettizia l'attività di controllo attuata al fine di verificare o evitare l'esecuzione di condotte illecite. Quindi in tutti quei casi in cui si presume che un lavoratore possa eseguire comportamenti penalmente rilevanti o integrare attività fraudolente nonché fonti di danno per l'azienda, è possibile il ricorso a investigatori privati. Diversamente le attività compiute, possono ritenersi, nel migliore dei casi, non ammissibili in giudizio e, molto spesso, illecite, configurando dei veri e propri reati che talvolta possono essere addirittura perseguiti d'ufficio. Pertanto, per poter raccogliere prove valide in giudizio è necessario affidarsi a società esterne munite dell'apposita licenza per svolgere le attività investigative prescritte dalla legge. Ma quali sono le indagini che possono essere svolte? In che modo si sostanzia il lavoro di un investigatore privato? Si tratta principalmente di controlli occulti, che vengono eseguiti tramite attività di osservazione, controllo e pedinamento, anche tramite l'utilizzo di tecnologie investigative evolute, come ad esempio il **Gps** *(Global positioning system,* sistema per la determinazione delle tre coordinate geocentriche relative alla posizione di un punto posto sulla superficie terrestre), ma non solo. In casi estremi, è addirittura possibile installare delle telecamere nascoste per documentare la condotta illecita del lavoratore, come spiegherò più avanti.

Dallo scopo personale alla rivendita delle informazioni

I casi reali sono molteplici e sconfinano dall'immaginazione comune, ma possono essere ricondotti fondamentalmente a non molte fattispecie. Infatti, vengono generalmente sottratte alle aziende informazioni, dati, brevetti e procedure che possono servire al lavoratore per due ragioni.
La prima è quella di mettersi in proprio o far mettere in proprio un familiare o ancora una persona molto vicina a lui, fondamentalmente per uno scopo personale. Se il soggetto sta perseguendo questa finalità è indispensabile poter dimostrare, con prove utilizzabili, tutti gli elementi che lo vedono coinvolto, sia personalmente che riconducendo a lui le aziende create. Se l'idea è quella di sottrarre informazioni, dati, brevetti, clienti o anche fornitori per poi utilizzarli per creare un'attività in concorrenza, le investigazioni dovranno essere svolte sia prima che successivamente. Prima per trovare tutti gli elementi utili a de-

L'autore

Nato a Milano, **Fabio Di Venosa** è un investigatore privato specializzato in investigazioni aziendali, indagini informatiche e nella ricerca di informazioni confidenziali. Ha fondato a Milano nel 2005 il **Centro Servizi Investigativi**, agenzia che svolge investigazioni sia in campo aziendale che privato. Dal 2020 l'agenzia è presente anche con una sede a Roma. All'interno di **Federpol** è stato vicepresidente per la regione Lombardia e Responsabile dell'Ufficio Stampa. Dal 2023 Di Venosa è responsabile Area Sicurezza di Osservatorio Metropolitano di Milano.

È sempre più frequente che all'origine di un incidente o di una violazione della privacy vi sia la condotta di un singolo dipendente infedele per ragioni diverse o, più semplicemente, inadempiente alle istruzioni impartitegli dal datore di lavoro. Le storie sintomatiche di questo fenomeno sono le più diverse: dal funzionario di banca che, per denaro, amicizia o amore, consegna a chi non dovrebbe informazioni bancarie di un correntista, al medico ficcanaso che accede ai fascicoli sanitari di pazienti non suoi per finalità diverse dalla cura, fino al principe di tutti i dipendenti infedeli, quello che, a qualche giorno dalla sua uscita dall'azienda presso cui lavora, si fa una copia dell'intero database dei clienti di quest'ultima per utilizzarli per farle concorrenza sleale.

terminare la sottrazione, per cristallizzare situazioni compromettenti e collusioni interne. Successivamente, invece, sarà importante scoprire i nessi fra le nuove aziende e il soggetto, ma non solo, si dovrà acclarare l'utilizzo di tutte quelle informazioni e dati sottratti per poter agire nei suoi confronti.
La seconda ragione è quella di arricchirsi, andando a rivendere quanto indebitamente sottratto. In questo caso il dipendente cederà le informazioni a società concorrenti a fronte di denaro, ma potrebbe succedere anche per avere benefici e favori. Anche in questo caso le indagini dovranno dapprima andare a dimostrare il furto e successivamente il passaggio di denaro o le possibili regalie e benevolenze ricevute dall'azienda concorrente. In entrambe le fattispecie è possibile operare nello stesso modo.

Controlli, pedinamenti e uso di telecamere

Andando nello specifico, è bene sapere che un dipendente infedele molto spesso si assenta dal lavoro, sia in orario lavorativo senza un giustificato motivo, che mettendosi in malattia, richiedendo ferie o permessi al fine di potersi recare dall'azienda concorrente o per porre in azione attività di concorrenza sleale personalmente. Questo può avvenire tuttavia, molto più semplicemente, anche dopo l'orario lavorativo oppure nei fine settimana. Pertanto, è indispensabile pedinare il lavoratore per poter documentare ciò che avviene, chi incontra e che cosa fattivamente avviene. Successivamente, in base a quanto scoperto, si procederà a raccogliere ulteriori informazioni tramite diversi canali e diverse attività di indagine per poter avere ulteriori elementi e un quadro completo della situazione. È molto importante porre attenzione a dettagli che potrebbero far presagire l'infedeltà del dipendente come malumori e litigi, nonché "rumors" riferiti da colleghi, questo al fine di poter predisporre dei controlli difensivi che per loro natura possono essere più pervasivi. Infatti, qualora il datore di lavoro abbia il fondato sospetto della commissione di illeciti ad opera del lavoratore può far predisporre, da un'agenzia investigativa, addirittura un controllo mediante telecamere occultate. Questo non al fine di misurare la prestazione lavorativa, di cui non verrà messo a conoscenza dagli investigatori, ma solo per documentare le azioni illecite e acquisire le informazioni utili per poterle dimostrare. Partendo da questa azione, che a volte è esauriente e definitiva, ci si procurano gli indizi per poter proseguire le indagini che a loro volta porteranno a delineare i fatti e tutta la situazione. Tutte le attività investigative, una volta giunte al termine, vengono documentate mediante una relazione dettagliata che racchiude tutti gli accadimenti comprensiva di fotografie e a volte anche filmati. La relazione investigativa ha valore probatorio in giudizio e gli investigatori che hanno svolto le indagini possono essere chiamati a testimoniare per confermare quanto visto e fornire, eventualmente, ulteriori elementi e dettagli.

Crisi di impresa e insolvenza

Dall'analisi del "Codice della crisi d'impresa e dell'insolvenza" emergono prospettive e opportunità per l'attività investigativa e ispettiva.

di Antonio De Matteis

Il decreto legislativo 12 gennaio 2019 n. 14, più noto come "Codice della crisi d'impresa e dell'insolvenza", attuativo della legge delega 19 ottobre 2017 n. 155, entrato in vigore solo il 15 luglio 2022 dopo una serie di integrazioni e modifiche, rappresenta una importante novità nel nostro ordinamento andando a sostituire la cosiddetta *"legge fallimentare"*. La ratio dell'impianto normativo è quella di anticipare l'intervento regolatore allo scopo di collocare lo scenario "fallimentare" quale soluzione estrema. In tale ottica il codice individua una fase

essenziale per la vita dell'impresa nella continua analisi delle dinamiche economiche aziendali, così da potere prevedere - con certo anticipo - il sopraggiungere di problemi di insolvenza, o anche solo di sovraindebitamento; l'acquisizione delle informazioni che ne derivano possono consentire l'uso tempestivo di uno degli strumenti messi a disposizione dal codice, scegliendo quello più appropriato al caso che interessa, per raggiungere il risanamento dell'azienda, anche mediante ipotesi negoziali che consentano la continuità della stessa, limitando la liquidazione patrimoniale alle sole ipotesi per le quali non è rinvenibile alcuna soluzione alternativa.

La legge antisuicidio

Per una compiuta comprensione della effettiva portata di detto codice, e soprattutto dei possibili destinatari dei suoi effetti, va precisato che, ancorché sia definito *"Codice della crisi d'impresa e dell'insolvenza"*, nel suo corpo vi è una sezione dedicata anche al consumatore, oltre che a quei soggetti che, secondo la vecchia disciplina erano genericamente definibili *"non fallibili"*, oggi *"non liquidabili giudizialmente"*. Con una delle ultime modifiche apportate al testo prima della sua entrata in vigore è stato sostanzialmente trasfuso, seppur con alcune modifiche, il contenuto della Legge n. 3 del 2012, più nota come *"legge antisuicidio"*. È sicuramente patrimonio della memoria di tutti che a seguito della crisi economica che ha colpito il nostro Paese, e non solo, fossero frequenti le notizie di suicidi di persone (imprenditori, professionisti o anche semplici consumatori) che arrivavano all'estremo gesto in quanto non più in condizione di adempiere ai propri impegni finanziari; da qui la promulgazione della "legge antisuicidio" con la quale il legislatore ha introdotto alcuni strumenti che consentivano l'esdebitazione del malcapitato, così da offrirgli la possibilità di riprendere una vita dignitosa. Il codice in questione, con i suoi 391 articoli, è rivolto a tutti i soggetti che a qualsiasi titolo (persone giuridiche o fisiche) si vengano a trovare in una situazione di insolvenza, ovvero anche solo di sovraindebitamento. È sufficiente una veloce lettura del testo per rinvenire tra le righe vari momenti nell'ambito dei quali l'intervento dell'investigatore potrebbe essere opportuno, per non dire di fondamentale importanza.
Prima di qualche esemplificazione, è opportuno precisare che ci si trova nell'ambito di attività fondamentalmente civilistica, e che il codice non disciplina forme di attività investigative; diretta conseguenza è che, mancando una previsione specifica (a differenza di quanto previsto in ambito penalistico, ove vi sono norme che disciplinano espressamene l'attività investigativa privata), si dovranno valutare di volta in volta le modalità con le quali le prove acquisite potranno essere utilizzate.

Gli strumenti disciplinati

Come già anticipato, il codice disciplina diversi strumenti tra i quali la *"composizione negoziata"*, la *"ristrutturazione dei debiti del consumatore"*, il *"concordato minore"*, la *"liquidazione controllata del sovraindebitato"* e altro ancora. La ristrutturazione dei debiti, riservata esclusivamente al consumatore sovraindebitato, consente la formulazione di un piano che indichi in modo specifico tempi e modalità per superare la crisi da sovraindebitamento; nella predisposizione di tale piano è possibile falcidiare anche i debiti muniti di privilegio, pegno o ipoteca, in misura non superiore a quanto realizzabile in ipotesi di liquidazione del bene oggetto della prelazione. Naturalmente presupposto per l'ammissione è la meritevolezza del debitore, nel senso che la posizione debitoria non deve essere stata provocata con colpa grave, malafede o addirittura con atti in frode dei terzi. Nell'ambito della procedura in questione un fattore che talvolta può assumere particolare rilevanza è dato anche dalla condotta tenuta dal finanziatore; la norma dispone, tra l'altro, che il creditore che abbia colpevolmente determinato la situazione di indebitamento, o il suo aggravamento, non può presentare opposizione o reclamo alla proposta formulata dal debitore.

L'autore

Avvocato cassazionista del Foro di Messina, **Antonio De Matteis** esercita la libera professione occupandosi prevalentemente di questioni di diritto amministrativo, civile e comunitario. Consigliere dell'Ordine degli Avvocati di Messina dal 2019 con la delega alle questioni di diritto amministrativo e alle Adr. Quale esperto in materia di giustizia complementare (in particolare mediazione civile e commerciale e composizione della crisi da sovraindebitamento) è stato docente di corsi di formazione, relatore in convegni e autore di diverse pubblicazioni.

Esistono diversi momenti nell'ambito dei quali l'intervento dell'investigatore potrebbe essere opportuno, per non dire di fondamentale importanza. Trovandosi però nell'ambito di attività fondamentalmente civilistica, dove il codice non disciplina forme di attività investigative, ne consegue che, mancando una indicazione specifica, si dovranno valutare di volta in volta le modalità con le quali le prove acquisite potranno essere utilizzate.

Il ruolo dell'apporto investigativo

Già dalla sintetica descrizione della procedura emergono alcuni degli ambiti nei quali l'apporto investigativo può essere determinante talvolta per il creditore, talaltra per il debitore (oltre che per l'attività svolta dal gestore della crisi). Si pensi ad esempio al profilo della meritevolezza; è di tutta evidenza che ciascun creditore può avere interesse ad accertare l'eventuale presenza della colpa grave, della mala fede ovvero della presenza di atti in frode, al fine di proporre al giudice motivate osservazioni avverso l'omologa del piano. Di contro il debitore potrebbe avere interesse a dimostrare l'eventuale colpa del creditore nella determinazione della situazione debitoria, così da inibirgli la proponibilità di opposizione o reclamo. Quanto detto per la ristrutturazione dei debiti, per grandi linee può valere anche per il concordato minore; riservato al professionista, all'imprenditore minore, all'imprenditore agricolo, e genericamente ad ogni debitore non assoggettabile alla liquidazione giudiziale, il concordato minore è utilizzabile dal soggetto che si trova in stato di sovraindebitamento per formulare ai creditori una proposta che gli consenta - in uno - di proseguire l'attività imprenditoriale/professionale e di superare la crisi.

Funzione ben diversa è rinvenibile nella liquidazione controllata; a differenza degli strumenti appena citati, volti a garantire la continuità aziendale o comunque la dignità della vita mediante una rimodulazione della posizione debitoria, in questo caso l'obiettivo è di mettere a disposizione dei creditori tutto quanto di cui dispone il debitore. Anche nell'ambito di tale procedura vi sono diversi spazi nei quali una compiuta attività investigativa potrebbe essere determinante per l'esito. Si pensi, ad esempio, all'ammissibilità della procedura liquidatoria su richiesta del creditore, procedura condizionata alla presenza di debiti scaduti non inferiori a 50.000 euro. Un creditore che abbia un credito inferiore a detta misura potrebbe ben avere interesse ad accertare se il debitore abbia ulteriori posizioni già scadute che, cumulate con la propria, superino detto limite al fine della procedibilità. In ultimo, si consenta un brevissimo accenno alla procedura di esdebitazione del sovraindebitato incapiente che consente alla persona fisica meritevole, che non sia in grado di offrire alcuna utilità, nemmeno in prospettiva futura, di esdebitarsi; tale procedura prevede la condizione che, ove il beneficiario nei successivi quattro anni dovesse acquisire utilità che consentano il soddisfacimento dei creditori in misura non inferiore complessivamente al 10%, debba metterli a disposizione della massa attiva. È evidente l'interesse dei creditori di conoscere se tale condizione si dovesse verificare.

In conclusione, nel fare presente che questo scritto non vuole essere una trattazione esaustiva del tema affrontato, ma semplicemente un input ad approfondire questo nuovo impianto normativo, si tiene evidenziare come, anche in questi ambiti giuridici, una fattiva collaborazione tra avvocato e investigatore può rappresentare la chiave vincente per il comune cliente.

Anpr: l'accesso negato

Tra le tante problematiche affrontate giornalmente dagli investigatori privati c'è quella del mancato accesso all'Anagrafe Nazionale della Popolazione Residente. Di seguito alcuni aspetti della questione e la proposta di eventuali soluzioni a cui Federpol sta già da tempo lavorando.

di Alfredo Passaro

Tra le tante questioni dibattute e che coinvolgono il delicato lavoro svolto dalla categoria professionale degli investigatori privati, ritengo che sia di estremo e attuale interesse la procedura di accesso online al cosiddetto **Anpr**, acronimo di *Anagrafe Nazionale della Popolazione Residente,* che, allo stato, è precluso agli investigatori privati dal Ministero dell'Interno.

Partiamo da concetti basilari, di sicuro conosciuti da tutti, per affrontare correttamente il problema. Per prima cosa va ribadito che l'Anpr è la banca dati unica del Viminale che favorisce lo scambio delle informazioni tra Comuni e pubbliche amministrazioni, nonché tra Comuni e cittadini. Nel gennaio 2022, i Comuni italiani hanno infatti completato la migrazione delle proprie anagrafi nell'Anpr, per cui i dati anagrafici della quasi totalità dei cittadini sono registrati e aggiornati dai Comuni nell'Anpr, banca dati definita unica, digitale e protetta. Dalla stessa banca dati si possono scaricare 14 diverse tipologie di certificati digitali in modo

autonomo e gratuito, senza dimenticare la possibilità di inviare la dichiarazione di cambio di residenza senza passare agli sportelli fisici, sia per trasferimenti all'interno dello stesso comune, sia per cambi di residenza tra Comuni differenti, sia per rimpatriare in Italia.
Tra i certificati che vengono rilasciati online dai Comuni all'utenza troviamo:

- **Certificato Anagrafico di nascita**
- **Certificato Anagrafico di matrimonio**
- **Certificato di Cittadinanza**
- **Certificato di Esistenza in vita**
- **Certificato di Residenza**
- **Certificato di Residenza Aire**
- **Certificato di Stato civile**
- **Certificato di Stato di famiglia**
- **Certificato di Stato di famiglia e di stato civile**
- **Certificato di Residenza in convivenza**
- **Certificato di Stato di famiglia Aire**
- **Certificato di Stato di famiglia con rapporti di parentela**
- **Certificato di Stato Libero**
- **Certificato Anagrafico di Unione Civile**
- **Certificato di Contratto di Convivenza.**

Come si vede, la politica della *"digitalizzazione della Pubblica Amministrazione"* sta dando i suoi frutti, mettendo nella concreta possibilità di eliminare l'utilizzo dello sportello fisico con la sostituzione di un cosiddetto *"sportello virtuale"* con sicuri vantaggi in termini di tempo e di costi diretti e indiretti che determinava sicuramente il rilascio della certificazione cartacea presso le sedi degli uffici anagrafe dei Comuni. Un notevole passo avanti, non c'è dubbio! Sennonché, come spesso accade nel nostro Paese, un passo in avanti è sempre accompagnato da due passi indietro, incomprensibili e totalmente irrazionali.
Infatti, la disciplina, così come articolata dai Ministeri competenti di concerto con l'Autorità Garante della protezione dei dati, prevede che l'accesso on-line per il rilascio della certificazione possa essere fatto solo dal diretto interessato, oppure da un familiare stretto, visto che con provvedimento n. 367 del 14 ottobre 2021 la citata Autorità ha espresso il proprio parere *"sullo schema di decreto recante le Modalità di erogazione da parte di ANPR dei servizi telematici per il rilascio di certificazioni anagrafiche online e per la presentazione online delle dichiarazioni anagrafiche"* specificando, tra l'altro che *"[...] il servizio consente all'iscritto in ANPR di richiedere il rilascio di un certificato esclusivamente per sé stesso o uno dei componenti della propria famiglia anagrafica (art. 2, comma 2)"*, escludendo, quindi, tutte quelle categorie professionali che sono autorizzate, per ragione della propria attività, a richiedere e ottenere lecitamente le certificazioni anagrafiche.

La fruizione del servizio da parte degli avvocati

A fronte di tale situazione normativo-amministrativa, alcuni Ordini professionali, con particolare riguardo a quello di cui faccio parte, hanno intrapreso l'iniziativa di consentire un agile accesso alla giustizia tramite apposite convenzioni per l'accesso telematico alla banca dati dell'Anagrafe Nazionale della Popolazione Residente per esigenze legali e di giustizia. Sono state in tal senso definite regole comuni applicabili alla fruizione del servizio a disposizione degli avvocati iscritti agli Ordini già prima dell'istituzione dell'ANPR. Attraverso tali convenzioni a suo tempo stipulate, detti professionisti, con tale *"accesso privilegiato"* per il rilascio di certificati anagrafici in via telematica, potevano interrogare il sistema di certificazione per ottenere tutte le informazioni necessarie allo svolgimento dell'attività a tutela dei diritti dei cittadini. Sembra ovvio che l'accesso, già consentito in presenza presso gli sportelli fisici non faceva altro che sostituirsi a quello telematico senza che lo stesso andasse a detrimento della tutela della privacy dei cittadini, ma velocizzando, contemporaneamente, la giustizia e le attività collegate, come quella degli investigatori privati riconosciuti appieno nel sistema giustizia anche in Italia, e nondimeno aiutando i Comuni e gli Uffici dell'anagrafe, con la ovvia riduzione circa l'accesso fisico, che altrimenti sarebbe necessario. Numeri alla mano parliamo, solo per fare l'esempio di Milano, di più di 700.000 accessi online a questo servizio per favorire la velocità delle attività a tutela dei cittadini attraverso la giustizia.

L'autore

Alfredo Passaro
è avvocato ed è specializzato in diritto amministrativo, con una rilevante attenzione alla materia degli appalti pubblici, alle autorizzazioni di polizia, nonché nella disciplina della tutela dei dati personali.

Però Il problema è sorto quando con la circolare 115 del 31 ottobre 2022, il Dipartimento per gli Affari Interni e Territoriali del Ministero degli Interni ha precisato che *«è esclusa la possibilità per il richiedente di acquisire, accedendo alla piattaforma Anpr con la propria identità digitale, certificati relativi a soggetti terzi»*. Tale situazione è stata posta all'attenzione del Ministero dell'Interno sia dagli ordini forensi che dalla Federpol, la quale ha intrattenuto contatti e effettuato incontri per spingere l'Amministrazione a modificare la propria posizione. Ebbene, mentre, allo stato, il Ministero dell'Interno non ha ritenuto di prendere una posizione nei confronti della categoria degli investigatori privati, nei riguardi dell'Ordine forense le cose sono andate diversamente, visto che dopo una formale presa di posizione dei Presidenti dei quattro Ordini più numerosi di Italia (Milano, Torino, Roma e Napoli) i quali hanno richiesto di rivedere la posizione assunta con una lettera al Ministro dell'Interno, il dottor **Matteo Piantedosi**, e al Viceministro dell'Interno, l'avvocato **Nicola Molteni**, nel marzo del 2023 è intervenuto un accordo di adesione tra il Viminale e il Consiglio nazionale forense che prevede l'interoperabilità dei sistemi informativi tra l'albo degli avvocati e la piattaforma e il Consiglio Nazionale Forense; ufficializzando tale convenzione, si evidenzia che con essa si perviene alla *"[...] soluzione di un problema fortemente avvertito dalla professione forense; gli avvocati avranno a disposizione i dati aggiornati di oltre 65 milioni di cittadini, inclusi i residenti all'estero, di cui potranno richiedere i certificati al fine di svolgere investigazioni difensive o per far valere e difendere un diritto in sede giudiziaria, in esenzione di bollo come previsto dalla legge".*

L'importanza di una convenzione

E per quanto riguarda gli investigatori privati? La risposta non può che essere: adesso tocca a voi! Nel senso che il Ministero ha dovuto riconoscere che per questioni di giustizia e per l'espletamento di attività investigativa risulta legittimo, e anzi necessario, autorizzare tutte le categorie professionali che per i motivi appena evidenziati necessitano di acquisire i certificati anagrafici. Occorre, quindi, sensibilizzare il predetto Dicastero facendo rilevare che non vi sono differenze – né potrebbero esserci – con la classe forense, visto che, peraltro, l'autorizzazione per l'espletamento delle investigazioni private viene rilasciata dall'organo periferico del Ministero dell'Interno (Prefetto) e che l'attività degli investigatori privati è soggetta a controllo costante e periodico da parte dello stesso apparato istituzionale oltre che dalle forze dell'ordine all'uopo deputate. Occorre, a mio avviso, accelerare gli sforzi dell'Associazione senza trascurare anche ulteriori *"azioni"* di intervento giudiziario, oltre che politico. Un dato è certo: non si può tollerare una tale limitazione quando non vi sono elementi che la giustificano, né ci si può celare dietro una generica *"tutela della privacy"*, visto che la categoria è stata ampiamente soggetta a tutta la relativa disciplina comunitaria e che gli adempimenti che vengono fatti dagli investigatori privati sono ampiamente in linea con le direttive, nazionali e comunitarie, in merito al trattamento dei dati. Quindi, se per gli avvocati è stato superato il limite indicato dall'Autorità Garante sopra indicata, allora anche per gli investigatori privati deve essere utilizzata la stessa misura, addivenendo ovviamente alla stipula di una altrettanta convenzione con **Federpol**, l'Associazione che rappresenta la quasi totalità degli investigatori privati italiani.

Non si può tollerare una tale limitazione quando non vi sono elementi che la giustificano, né ci si può celare dietro una generica "tutela della privacy", visto che la categoria è stata ampiamente soggetta a tutta la relativa disciplina comunitaria e che gli adempimenti che vengono fatti dagli investigatori privati sono ampiamente in linea con le direttive, nazionali e comunitarie, in merito al trattamento dei dati.

L'attuazione della direttiva "whistleblowing"

L'Italia ha recepito in via definitiva la direttiva europea sul "whistleblowing". La tutela del "whistleblower" è un diritto fondamentale, riconosciuto a livello internazionale, e rappresenta un'estensione del diritto di libertà di espressione. Le principali novità di questa normativa sono qui sintetizzate.

di Elisabetta Busuito

Con il D.Lgs. n. 24/2023, attuativo della direttiva UE n. 2019/1937, si è ridisegnato il sistema di protezione delle persone (cosiddetti *whistleblowers*) che segnalano violazioni di disposizioni del diritto europeo e/o nazionale, lesive dell'interesse pubblico o dell'integrità dell'Amministrazione Pubblica o del privato, di cui siano venuti a conoscenza nel proprio contesto lavorativo.
Le principali novità di questa normativa possono essere così sintetizzate:

i) ampliamento dei destinatari degli obblighi organizzativi e di protezione, dei segnalanti e delle condotte potenzialmente illecite ritenute meritevoli di segnalazione;
ii) introduzione di un canale di segnalazione esterno affidato all'**Anac**, cui è stato assegnato un ruolo di garanzia e vigilanza, nonché il potere sanzionatorio;
iii) applicabilità delle misure di protezione del segnalante anche in caso di pubblica divulgazione delle violazioni ed elaborazione di efficaci protezioni dal rischio ritorsivo;
iv) stringente regolamentazione della riservatezza dell'identità del segnalante, delle modalità di gestione delle segnalazioni e di conservazione della relativa documentazione.

• Quali fatti possono esser segnalati?
Ampia è la nozione di violazione comprensiva, fra l'altro, di:

1) illeciti amministrativi, contabili, civili e penali di qualsiasi natura;
2) condotte illecite rilevanti ai sensi del Decreto 231/01 e violazioni dei Modelli di Organizzazione, Gestione e Controllo (cosiddetti Mog);
3) illeciti rientranti nell'ambito di applicazione degli atti dell'Unione europea o nazionali (puntualmente indicati nella Direttiva) e relativi a settori quali, ad esempio, la sicurezza e conformità dei prodotti o la tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi. Espressamente escluse dalla nuova disciplina sono, fra l'altro, le contestazioni afferenti esclusivamente i propri rapporti individuali di lavoro o di impiego pubblico, o quelli con i superiori gerarchici.

• Quali enti debbono uniformarsi a questa nuova disciplina?
I soggetti pubblici (Pubbliche Amministrazioni, Autorità Amministrative indipendenti di garanzia, vigilanza o regolazione, enti pubblici economici, concessionari di pubblico servizio, ecc.) e alcuni soggetti privati (enti che hanno impiegato nell'ultimo anno la media di almeno 50 lavoratori subordinati, con contratti a tempo indeterminato e non) e, indipendentemente dal numero medio di lavoratori, enti operanti in alcuni specifici ambiti enumerati negli allegati al Decreto e quelli che si erano già dotati di un Mog.

• Chi può effettuare la segnalazione?
Qualsiasi lavoratore del settore pubblico e privato, indipendentemente dal suo inquadramento (quindi anche gli autonomi, i consulenti, i volontari ecc.); la tutela apprestata per questi soggetti si estende, ed è una novità, anche a figure quali: i facilitatori (coloro che prestano assistenza al lavoratore nel processo di segnalazione), gli operatori del medesimo contesto lavorativo del segnalante o di chi ha sporto una denuncia o una divulgazione pubblica e che siano legati ad essi da uno stabile legame affettivo o di parentela entro il quarto grado; i colleghi che lavorano nello stesso contesto del whistleblower ed hanno con lui un rapporto abituale e corrente; gli enti di proprietà del segnalante o per i quali questi lavora, nonché quelli operanti nel medesimo contesto professionale.

• Quali sono i canali di segnalazione?
I canali sono due, uno interno all'ente ed un altro esterno che avrà come destinatario l'Anac. Quanto al primo, gli enti dovranno implementare (sentiti i sindacati), strumenti di trasmissione/ricezione delle segnalazioni che garantiscano, anche attraverso il ricorso alla crittografia, la riservatezza (i) dell'identità del segnalante, (ii) della persona coinvolta e di quella comunque menzionata nella segnalazione, (iv) del contenuto e della documentazione della stessa. A gestire il canale dovrà essere un soggetto interno o esterno, autonomo e specificamente formato.

• Come possono esser fatte le segnalazioni?
In forma scritta, anche con modalità informatiche, o orale (mercè linee telefoniche o messaggistica vocale) ovvero ancora, su richiesta del segnalante, tramite un incontro diretto. Innovativi gli oneri organizzativi posti in capo al gestore delle segnalazioni, che dovrà rilasciare al segnalante avviso di ricevimento entro sette giorni dalla ricezione; svolgere le più opportune attività istruttorie e, nel caso, chiedere integrazioni; fornire riscontro alla segnalazione entro tre mesi dall'avviso di ricevimento o, in mancanza, dalla scadenza del termine di sette giorni; dare informazioni chiare su canale, procedure e presupposti per fare le segnalazioni interne ed esterne (rendendole visibili nei luoghi di lavoro e, se esistente, sul sito web, nonché accessibili alle persone che, pur non frequentando i luoghi di lavoro, intrattengono un rapporto giuridico con l'ente); conservare la documentazione secondo quanto indicato nell'art. 14 del Decreto.
Inedita la possibilità per i whistleblower di trasmettere le segnalazioni all'Anac, attraverso un canale dedicato istituito dall'Anac, ma solo se ricorra una delle seguenti condizioni:

i) nel contesto lavorativo del segnalante l'attivazione del canale interno non sia obbligatoria, ovvero non sia attivo, o non costruito secondo i requisiti del Decreto;
ii) la segnalazione interna non ha avuto alcun séguito;
iii) il segnalante ha fondato motivo di rite-

Il decreto fissa un obbligo generale di riservatezza per cui le informazioni sulle violazioni non possono utilizzarsi oltre il necessario per dare loro séguito. Riguardo al segnalante, risulta granitico il divieto di rivelazione della sua identità a persone diverse da quelle competenti a ricevere o a dar seguito alle segnalazioni.

nere che una segnalazione interna non avrebbe séguito o lo esporrebbe a un rischio di ritorsione;

iv) la violazione segnalata può fondatamente ingenerare un pericolo imminente o palese per il pubblico interesse.

La divulgazione pubblica rappresenta un'ulteriore modalità di "denuncia", ma solo a certe condizioni (cui è subordinato il diritto di godere delle misure di protezione), e cioè che: (i) sia stata già effettuata rituale segnalazione interna ed esterna o direttamente esterna, senza esito; (ii) il segnalante non abbia fatto la segnalazione ricorrendo ai canali "ordinari" ritenendo che la violazione rappresenti un pericolo imminente o palese per il pubblico interesse; o ancora (iii) che il segnalante tema ragionevolmente che la segnalazione esterna possa esporlo a ritorsioni, o restare inefficace.

• Com'è disciplinata la riservatezza nel sistema del whistleblowing?

Il decreto fissa un obbligo generale di riservatezza per cui le informazioni sulle violazioni non possono utilizzarsi oltre il necessario per dare loro séguito. Riguardo al segnalante, risulta granitico il divieto di rivelazione della sua identità a persone diverse da quelle competenti a ricevere o a dar seguito alle segnalazioni (salvo consenso espresso dell'autore). Per quanto attiene ad eventuali procedimenti penali (aperti a valle della segnalazione), l'identità del segnalante è coperta da segreto secondo il disposto dell'art. 329 c.p.p. Le segnalazioni sono, inoltre, sottratte all'operatività degli istituti dell'accesso agli atti e dell'accesso civico.

• Quale tutela è stata normativamente prevista in favore dei segnalanti?

In primis va ricordato che la tutela scatta solo se la segnalazione è rispettosa delle modalità normativamente previste e, al momento della divulgazione o della denuncia, il segnalante fondatamente stimava le informazioni vere e rientranti nell'ambito oggettivo del Decreto. Le tutele si applicano anche in caso di segnalazione, denuncia o divulgazione anonime, se l'autore è poi identificato e ha subìto ritorsioni. La garanzia prima consiste nel divieto di ogni forma di ritorsione a danno del segnalante e nella nullità di qualsiasi atto ritorsivo, in uno con la reintegra nel posto di lavoro in caso di licenziamento. Nei procedimenti giudiziari concernenti atti o omissioni ritorsivi si realizza un'inversione dell'onere probatorio, nel senso che si presume che gli stessi siano stati posti in essere a causa della segnalazione. Merita, infine, ricordare che il whistleblower può comunicare le ritorsioni subìte all'Anac che ne informerà il Dipartimento della Funzione Pubblica o l'Ispettorato Nazionale del Lavoro. Nessuna tutela sarà accordata ove accertata, anche non in via definitiva, la responsabilità del segnalante per diffamazione, calunnia o altri reati commessi con la proposizione della denuncia o la sua responsabilità civile per lo stesso titolo, nei casi di dolo o colpa grave.

• Quali sono le sanzioni?

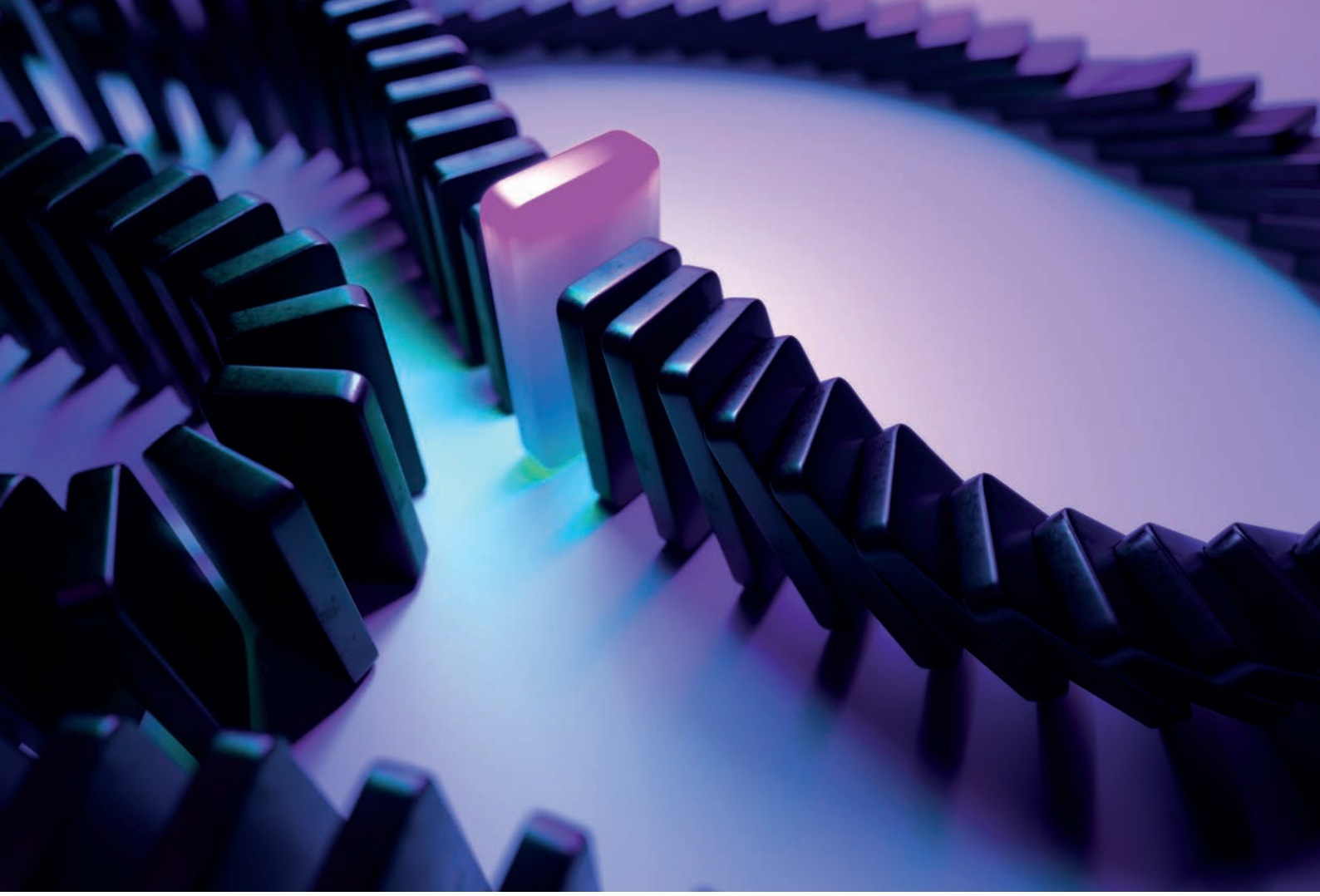
Per assicurare effettività alla nuova disciplina, è stato costruito un apparato sanzionatorio sul cui funzionamento vigilerà l'Anac. Le sanzioni vanno da 10.000 a 50.000 euro in caso, fra l'altro, di accertate ritorsioni, violazioni dell'obbligo di riservatezza, o non conformità del sistema di segnalazione; da 500 a 2.500 euro in caso di illecito penale o civile del whistleblower. Anche i privati dotati di Mog debbono ivi prevedere sanzioni verso i responsabili degli illeciti testé descritti.

• Da quando saranno efficaci le disposizioni del Decreto?

Dal 15 luglio 2023, salvo che per i privati che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, fino a 249 unità, per i quali ultimi l'obbligo scatta dal 17 dicembre 2023.

L'autrice

Elisabetta Busuito è avvocato patrocinante alle Corti Superiori. Assiste società, manager e imprenditori in procedimenti per reati societari, tributari, fallimentari, contro il patrimonio, la PA e la persona. Autrice di pubblicazioni nelle tematiche del diritto penale d'impresa, è partner e responsabile del dipartimento di Diritto Penale di **B-HSE Società tra Avvocati**.



L'importanza della "business continuity"

La gestione del rischio negli adeguati assetti organizzativi aziendali e lo stretto legame con gli obiettivi di sostenibilità.

di Milene Sicca

Pandemia, inflazione, aumento delle materie prime, credit crunch, crisi delle catene logistiche globali e instabilità geopolitica hanno messo a repentaglio la sopravvivenza di molte aziende. Alla luce di quanto sopra, gli orientamenti normativi nazionali e sovranazionali in tema di crisi e risanamento di impresa e di responsabilità degli organi apicali hanno maggiormente spinto verso la cultura della prevenzione e del risk approach. La salvaguardia della continuità aziendale passa dunque attraverso l'adozione degli adeguati assetti **Oac** *(Organizzativi, Amministrativi, Contabili)* che hanno imposto alle imprese nazionali, anche alle micro e alle Pmi che rappresentano oltre il 90% del perimetro nazionale, un notevole salto di qualità culturale nell'ottica di una gestione manageriale del proprio business qualunque ne sia la dimensione.
Ai criteri Oac si aggiunge inoltre il tema della sostenibilità sotto tutte le sue fattispecie, per cui la compliance aziendale ai criteri **Esg** *(Enviromental, Social, Governance)* che determinano un'ulteriore svolta, ben più profonda, complessa ed articolata. Di conseguenza, come si vedrà in seguito, l'evoluzione del concetto di affidabilità delle imprese dovrà approdare a quello,

più ampio, della sostenibilità aziendale. Per questi motivi è importante che gli imprenditori reagiscano tempestivamente adottando non solo adeguati assetti organizzativi aziendali di natura amministrativo contabile come previsto dall'art 2086 cc e richiamato dall'art 3 del D.Lgs. 14/2019 del *Codice della Crisi d'Impresa e Insolvenza* entrato in vigore lo scorso 15/07/2022, ma allarghino l'orizzonte di analisi dei rischi e delle opportunità implementando politiche e soluzioni di *"business continuity"* e *"business sustainability"*.

Il concetto di business continuity

Con la definizione business continuity si intende *"la capacità di un'azienda di proseguire le attività anche in condizioni di crisi, o comunque sotto l'esposizione di minacce attive"*. Dette minacce hanno natura sia endogena che esogena: non sono quindi determinate solo da incapacità amministrativo gestionali, ma anche da fattori esterni. Possiamo pertanto parlare di business continuity management come di quella serie di processi attraverso i quali l'azienda riesce a costruire e mantenere nel tempo le suddette capacità, per individuare con largo anticipo le minacce reali e potenziali, valutare le conseguenze sul business e identificare quali saranno le decisioni da prendere con le relative risorse umane ed economiche da impiegare. La continuità operativa comprende dunque la funzionalità dell'organizzazione nella sua interezza. Di conseguenza, la *"swot analysis"* deve necessariamente considerare le minacce derivanti da questi ambiti. Il mancato presidio, e quindi l'accadimento del rischio paventato, può avere effetti esiziali per l'impresa. In questo come in altri ambiti richiamati nel presente articolo, gli organi di controllo dell'impresa, che siano rappresentati sia dagli stessi esponenti sia da figure manageriali specifiche e/o da Organismi di Vigilanza in caso di adozione di Modelli Organizzativi, per rendere più pregnante e incisiva l'azione di controllo e monitoraggio dei rischi possono avvalersi dell'ausilio strategico delle capacità offerte dagli Istituti di Investigazione e Informazione autorizzati.

Le principali aree di rischio

Secondo la **Eciia** *(European Confederation of Institutes of Internal Auditing)*, i principali fattori di rischio esogeno ed endogeno che possono minare la continuità aziendale sono molteplici e con una perniciosità potenziale destinata a crescere. L'indagine *"Risk in Focus 2023"* di Eciia ha tracciato, classificandole per gravità, le principali aree di rischio destinate a influenzare le scelte strategiche delle imprese elencate di seguito.

1. **Sicurezza informatica e sicurezza dei dati**
2. **Capitale umano, diversità e gestione dei talenti**
3. **Incertezza macroeconomica e geopolitica**
4. **Modifica di leggi e regolamenti**
5. **Trasformazione digitale, nuove tecnologie e intelligenza artificiale**
6. **Cambiamenti climatici e sostenibilità ambientale**
7. **Continuità aziendale, gestione delle crisi e gestione delle emergenze**
8. **Filiere fornitori, appalti e rischio d'appalto**
9. **Rischi finanziari, di liquidità e di insolvenza**
10. **Gestione organizzativa e rendicontazione aziendale.**

Il rapporto esplora una serie di temi, tra cui l'incertezza geopolitica e macroeconomica, il cambiamento climatico e la sostenibilità ambientale, la cultura organizzativa, la sicurezza informatica e dei dati, la digitalizzazione e l'intelligenza artificiale, il rischio di default, le filiere, il rischio di contaminazione mafiosa, ecc. Ci sono poi ulteriori fattori che negli ultimi anni abbiamo imparato a considerare e sono i cosiddetti "cigni neri", che corrispondono a quegli accadimenti dei quali a priori è impossibile prevederne il realizzarsi, quali ad esempio la pandemia di Covid-19 la cui magnitudo ha avuto un impatto devastante a livello mondiale non solo sulla salute delle persone ma, per il suo perdurare, soprattutto a livello economico. Abbassando la gradazione di imprevedibilità dobbiamo considerare altre categorie di fattori che possono impattare sulla continuità aziendale e sono dati dai cosìddetti "rischi fisici" dettati dall'ubicazione geogra-

L'autrice

Milène Sicca
è Presidente del Comitato Studi Legislativi di **Federpol** e amministratore di **GIB Italia Service**, società che da oltre 30 anni si occupa di indagini patrimoniali, recupero e tutela del credito. È anche docente presso l'Università Mercatorum di Roma.

fica per quelle attività che si trovano per esempio in aree a rischio sismico, alluvioni, esondazioni, frane, rischio termico, rischio vulcanico ecc. Non è dato sapere quando e come quel determinato evento potrà realizzarsi, ma di converso è possibile prevedere misure adeguate al contenimento del rischio. I rischi fisici sopramenzionati sono contemplati anche nelle politiche legate alla sostenibilità e ai fattori Esg richiamate al punto 6 della tabella Risk and Focus 2023 e sono destinati a salire rapidamente in graduatoria nei prossimi anni.

Le imprese e la sostenibilità

Cambiamenti climatici e sostenibilità ambientale sono diventate una delle aree più dinamiche e in rapida evoluzione che le aziende dovranno integrare nel proprio business per garantirsi condizioni di continuità e solidità nel lungo periodo. Sono molti gli stakeholders interni ed esterni all'impresa che sollecitano la responsabilità e la trasparenza delle performance ambientali, sociali ed economiche. Le organizzazioni non devono considerare la sostenibilità come un mero esercizio di conformità e una **Dnf** *(Dichiarazione non finanziaria collegata al bilancio d'esercizio)* poco sentita e veritiera. Al contrario, l'applicazione dei principi Esg fornisce alle aziende la solidità e trasparenza di cui hanno bisogno, anche per evitare rischi reputazionali derivanti dalle accuse di *"greenwashing"* e soprattutto per assicurare agli stakeholder che l'organizzazione è sulla strada giusta per raggiungere obiettivi tangibili nelle performance Esg, quali ad esempio il *"net-zero"* (abbassamento/abbattimento delle emissioni di carbonio e di sostanze climalteranti).
In Italia l'obbligo di redazione del bilancio di sostenibilità, alias **Dnf** *(Dichiarazione Non Finanziaria)* e i relativi adeguamenti è partito col D.Lgs. 254/2016 a recepimento della Direttiva Europea 2014/95, dapprima per grandi imprese, gruppi di grandi dimensioni e quotate, in quanto considerate enti di interesse pubblico (banche, assicurazioni, società quotate ecc.) con oltre 500 dipendenti e uno stato patrimoniale superiore a 20 milioni o ricavi di almeno 40 milioni. Tali società sono tenute a presentare una dichiarazione di carattere non finanziario, in cui devono essere riportate informazioni ambientali, sociali, attinenti al personale, al rispetto dei diritti umani, alla lotta contro la corruzione attiva e passiva in misura adeguata alla salvaguardia della compliance aziendale e dei suoi risultati nel tempo. Allo stato attuale con la **Csrd/2022** *(Corporate Sustainability Reportig Disclosure)* la soglia dei 500 dipendenti si è dimezzata e l'applicazione dei criteri di sostenibilità è destinata ad allargarsi progressivamente a macchia d'olio in tutti i settori dell'economia e, quindi, a scendere verso tutti i livelli dimensionali delle imprese in quanto diretti interessati o facenti parte delle filiere connesse. L'obiettivo è quello di garantire la massima trasparenza e affidabilità di fronte agli stakeholder. Nel caso in cui alcuni ambiti previsti dalla Dnf non siano presidiati, l'azienda è obbligata a fornirne le motivazioni anche in caso di irrilevanza. Le informazioni esposte devono rispondere a standard riconosciuti a livello internazionale, tra cui quelli **Gri** *(Global Reporting Initiative).*
In particolare, le imprese non finanziarie nella Dnf devono pubblicare informazioni su:

- **quota di fatturato proveniente da prodotti o servizi associati ad attività economiche allineate alla tassonomia;**
- **quota di spese in conto capitale (Capex) e di spese operative (Opex) relative ad attivi o processi associati ad attività economiche allineate alla tassonomia.**

Allo stato attuale, banche e intermediari finanziari hanno già cominciato il processo di adeguamento che prevede la pubblicazione dei propri indicatori chiave di performance o Kpi *(Key Performance Indicator)* che esprimono la percentuale di allineamento alla tassonomia degli asset in gestione. In questo caso, il Kpi è rappresentato come un rapporto tra investimenti e attività finanziarie allineati alla tassonomia (al numeratore) e totale degli investimenti e delle attività finanziarie (al denominatore). Poiché la "finanza tradizionale" deve lasciare il passo alla "finanza sostenibile" (in altri termini, i capitali non destinati a "rendere sostenibili" le attività aziendali si ridurranno sostanzialmente nei prossimi anni), è evidente che anche le imprese non finanziarie direttamente interessate, per dimensione e caratteristiche, dalle norme vigenti, nonché quelle aventi causa con le precedenti per

In ambito aziendale la cultura della rilevazione, del presidio e della riduzione dei rischi specifici interni ed esterni, assume rilevanza centrale ai fini dell'orientamento e dell'organizzazione, con riflessi positivi in termini di sicurezza, trasparenza e continuità.

catene di fornitura, non possano rinviare il proprio adeguamento alla transizione.

Le filiere dei fornitori in ambito Esg

Un altro aspetto fondamentale riguarda la sostenibilità della supply chain, nei tre pillar Esg ambientale, sociale ed economico, a cui banche e grandi appaltatori della Pubblica Amministrazione stanno già guardando con attenzione, volendo garantire la compliance della catena di fornitura anche ai singoli fornitori e ai fornitori dei fornitori in modo capillare, affinché coprano tutte le tematiche legate alla sostenibilità attraverso l'intera supply chain. Nessuna azienda potrà infatti diventare e dichiararsi veramente sostenibile senza affrontare la sfida con tutta la propria filiera.

Le verifiche preventive

Una corretta e responsabile governance dell'impresa non può prescindere da una serie di verifiche preventive la cui inosservanza potrebbe compromettere in modo esiziale la continuità d'impresa per le molteplici fattispecie di rischio civile e penale o più gravemente dalla contaminazione esterna delle organizzazioni criminali nell'ambito delle filiere di fornitura. Anche in questo caso l'Odv, o chi per esso, per rendere più incisivo e capillare il controllo, può avvalersi con successo di attività informative e investigative sondando la solvibilità dei fornitori, raccogliendo informazioni e prove sul territorio, oltre a effettuare le verifiche antiriciclaggio nelle banche dati o con strumenti Osint, a intercettare possibili situazioni di corruzione, a ricercare eventuali legami diretti e indiretti con esponenti della criminalità organizzata, questo al fine di contrastare l'applicazione delle misure di prevenzione antimafia ex art 34 e o quella più mite di controllo ex 34 bis D.Lgs. 159/2011. Infatti, l'art 34 bis *ai punti d) ed e) prev*ede che nell'ambito della bonifica dell'azienda sottoposta a misura di controllo per contaminazione occasionale il Tribunale possa disporre:

d) di adottare ed efficacemente attuare misure organizzative, anche ai sensi degli articoli 6, 7 e 24–ter del decreto legislativo 8 giugno 2001, n. 231, e successive modificazioni;

e) di assumere qualsiasi altra iniziativa finalizzata a prevenire specificamente il rischio di tentativi di infiltrazione o condizionamento mafiosi.

Il ruolo dei modelli organizzativi

All'alba dell'entrata in vigore del D.Lgs.. 231/2001, l'adozione di **Mog** *(Modelli Organizzativi Gestionali aziendali)* era vista più come una sorta di scudo protettivo avverso la contestazione di responsabilità amministrativa/penale dell'ente per reati commessi nell'interesse e a vantaggio dello stesso da soggetti apicali o loro sottoposti. Con le modifiche apportate all'art 2086 c.2 dal D.Lgs. 14/2019 Ccii l'onere a carico di imprese ed enti di dotarsi di adeguati assetti organizzativi, si è trasformato in un vero e proprio obbligo di legge. Di conseguenza oggi si può affermare che i Mog, che potremmo definire come la riassunzione grafica e funzionale dell'organizzazione aziendale, sono ormai identificati come strumenti che sanciscono il principio di "adeguatezza nel governo societario". Nella formulazione originaria, il D.Lgs. 231/2001 prevedeva la responsabilità per gli enti in caso di commissione di alcuni reati, esclusivamente dolosi, attinenti ai rapporti con lo Stato e la Pubblica Amministrazione, quali l'indebita percezione di erogazioni, la truffa in danno dello Stato o di un Ente pubblico o per il conseguimento di erogazioni pubbliche, la frode informatica, la concussione e la corruzione. Nel corso degli anni la norma in parola ha subito numerose modifiche che hanno progressivamente ampliato il catalogo dei reati-presupposto, dalla cui commissione può scaturire la responsabilità dell'ente (si veda il riquadro).

Naturalmente i Mog, che al momento restano solo un'opzione consigliata e non obbligatoria, vanno considerati come un'opportunità per l'impresa che si voglia tutelare in via preventiva e voglia cogliere l'occasione per migliorare la propria organizzazione in una prospettiva evolutiva. Possiamo dire che i Mog, unitamente ai Codici Etici, fanno parte della più ampia famiglia dei *Compliance Programs* legati alla sostenibilità. Esiste infatti uno stretto legame tra gli obiettivi del Mog e i fattori Esg, tant'è che tra i reati enucleati dal D.Lgs. 231/2001 ci sono per esempio:

- **i reati ambientali contemplati dal pillar "E" Environmental;**
- **i reati contro la salute e sicurezza dei lavoratori, i reati legati ai lavoratori irregolari, i reati contro la personalità individuale ecc. contemplati dal pillar "S";**
- **i reati informatici, i reati di riciclaggio, i reati di corruzione, i reati tributari, i reati di contrabbando, i reati connessi in materia di mancata compliance al Gdpr, contemplati dal pillar "G".**

Possiamo trovare la sovrapposizione di molti obiettivi che accomunano la norma 231/2001 con i *"Goals"* dell'Agenda Onu 2030 in materia di sviluppo sostenibile. Tra i *"Sustainable Development Goals"* dell'Agenda 2030 si trovano, infatti, elementi quali *"Incentivare una crescita economica duratura, inclusiva e sostenibile, lavoro dignitoso, consumo e produzione responsabile, proteggere, ripristinare e favorire un uso sostenibile dell'ecosistema terrestre, pace, giustizia e istituzioni solide, ecc"*.

In ambito aziendale, la cultura della rilevazione, del presidio e della riduzione dei rischi specifici interni ed esterni, assume rilevanza centrale ai fini dell'orientamento e dell'organizzazione, con riflessi positivi in termini di sicurezza, trasparenza e continuità. Possiamo quindi concludere affermando che l'unione tra i principi di sostenibilità, sicurezza e una governance improntata a contribuire positivamente al futuro del pianeta, sia sicuramente la strada giusta per traghettare l'impresa ad essere essa stessa parte pulsante della transizione.

I Mog e i reati presupposto

Di seguito un riepilogo dei reati presupposto:

1. Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'Unione Europea per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture.
2. Delitti informatici e trattamento illecito di dati.
3. Delitti di criminalità organizzata.
4. Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio.
5. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento.
6. Delitti contro l'industria e il commercio.
7. Reati con finalità di terrorismo o eversione dell'ordine democratico previsti da codice penale e leggi speciali.
8. Delitti contro la personalità individuale.
9. Reati di abuso di mercato.
10. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
11. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché auto-riciclaggio.
12. Delitti in materia di strumenti di pagamento diversi dai contanti.
13. Delitti in materia di violazione del diritto d'autore.
14. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.
15. Reati ambientali.
16. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare.
17. Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati.
18. Reati tributari.
19. Reato di contrabbando-diritti di confine.
20. Delitti contro il patrimonio culturale.
21. Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici.
22. Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato.
23. Reati transnazionali.

Chi ha paura del cybercrime?

Il rafforzamento dell'attività di tutela dei sistemi informatici per contenere la minaccia cyber tra l'attuazione della Direttiva NIS 2 e l'istituzione dell'Agenzia per la Cybersicurezza Nazionale.

di Fabrizio Fratoni

Negli ultimi anni si sta registrando un esponenziale aumento della minaccia cyber che, con le accresciute potenzialità dei mezzi tecnologici, tenta di aggredire tutte quelle attività istituzionali ed economiche che fruiscono del web, dagli enti pubblici alle imprese, oltre che dei cittadini particolarmente vulnerabili nei confronti degli attacchi posti in essere dai criminali informatici.
Gli attacchi non sono più posti in essere da malfattori non strutturati, ma da centinaia di gruppi criminali transnazionali che operano nel *dark* e nel *deep web*, in condizioni di totale anonimato, orientati ad agire in maniera organizzata e strutturata e che hanno come obiettivo e campo di battaglia infrastrutture, reti, server, client, device mobili, oggetti IoT e piattaforme social su scala globale, 365 giorni all'anno. Il volume sempre crescente dei dati aziendali e delle informazioni personali archiviate nel cyberspazio, incoraggiato dal crescente ricorso al sistema cloud, rende l'attacco informatico potenzialmente molto redditizio e relativamente privo di rischi per l'attaccante. Non sorprende, quindi, che l'impatto economico della criminalità in-

formatica sia sempre più preoccupante; ciò è particolarmente rilevante e dannoso per Paesi come l'Italia, per i quali il furto di know-how scientifico, tecnologico e originale delle aziende del territorio, diviene un grave danno al vantaggio comparativo, minando la loro competitività sui mercati globali.

Anche per le tensioni geopolitiche, si registra in ambito internazionale una nuova fase di *"guerra cibernetica diffusa"*, che ha interessato anche il nostro Paese, il quale è stato oggetto nel 2022 di una recrudescenza di attacchi messi a segno, ben 188, in crescita del 169% rispetto all'anno precedente e circa il 7,6% (contro il 3,4% del 2021) degli attacchi globali. Anche l'analisi degli incidenti informatici avvenuti nel 2022 evidenzia una netta prevalenza di attacchi con finalità di cybercrime, che sono stati oltre 2.000 a livello globale, ovvero l'82% del totale, in crescita del 15% rispetto al 2021, e per l'Italia la percentuale sale al 93%, in crescita del 150% rispetto al 2021. Si osserva, inoltre, che la parte maggiore degli attacchi è stata diretta verso le aziende manifatturiere del Made in Italy, nel settore tecnico-scientifico e dei servizi professionali e che in oltre l'80% dei casi ha avuto conseguenze molto gravi per le imprese attaccate. Nel contesto della guerra tra Federazione russa e Ucraina, con le annesse tensioni internazionali tra superpotenze, il nostro Paese appare particolarmente sotto pressione, dato che la gravità delle azioni poste in essere dai criminali informatici è risultata elevata o critica nell'83% dei casi. Peraltro, gli attacchi nel nostro Paese sembrano andare di pari passo con il grado di maturità tecnologica negli specifici ambiti: i settori dei servizi professionali, e tecnico-scientifico registrano un incremento del 233,3% di incidenti gravi, l'industria manifatturiera il +191,7%, il comparto informatico con il +100% e governativo-militare con il+65,2%.

Il rafforzamento della cybersicurezza in Europa

Appare, quindi, necessario accrescere, in ogni ambito, il livello di tutela di tutte le attività che comunque interagiscono nel web sempre più esposte al cyber risk.

Quali sono le principali minacce cyber?

Possono distinguersi in tale ambito quattro tipi di minacce.

1 | Minaccia di cybercrime
Contempla tutte quelle attività dolose con intento criminale svolte nel cyberspazio, come truffe o frodi su Internet, furto di identità, furto di dati o di proprietà intellettuale che colpiscono imprese e utenti

2 | Minaccia di spionaggio informatico
Si sostanzia nell'acquisizione indebita di dati riservati, non necessariamente di valore economico o commerciale, ma che possono avere impatto sulla sicurezza di persone ed enti pubblici o privati, fino a quella dello Stato.

3 | Minaccia di cyber terrorismo
È finalizzato allo sfruttamento ideologicamente motivato delle vulnerabilità dei sistemi con l'intento di influenzare uno stato e/o un'organizzazione internazionale e/o un numero indeterminato di utenti della rete

4 | Minaccia cyber warfare
Si tratta di una minaccia relativa a quelle attività e operazioni svolte in ambito cyber per ottenere vantaggio operativo di rilevanza militare.

Una situazione che deve essere vista non solo come sfida da affrontare ma anche come opportunità da cogliere, che non può essere lasciata in secondo piano in ogni settore professionale; sia partendo dalle iniziative di prevenzione e contrasto poste in essere, sia in ambito europeo che in ambito nazionale, nel più ampio contesto di garantire lo spazio cibernetico, nel quale una molteplicità di attori a partire dallo specifico settore scientifico e tecnico professionale, fino dalle associazioni di categoria, sono chiamate a intervenire con l'obiettivo di incrementare la resilienza italiana e la capacità di risposta in caso di crisi cibernetiche. Proprio per rafforzare il livello di cybersicurezza nell'Unione, il legislatore europeo aveva già emanato la Direttiva 2016/11481/UE, denominata **Direttiva NIS 1**, che ha fissato i principi comuni da applicare nei singoli ordinamenti nazionali a cura dei Paesi membri, per sviluppare le capacità di resistenza dei sistemi informatici e di rete utilizzati per fornire servizi essenziali in settori chiave e garantire la continuità degli stessi in caso di incidenti. Ma tale direttiva era inapplicabile ad alcuni soggetti divenuti con il tempo centrali per il corretto funzionamento del mercato europeo, i quali più volte si sono dimostrati impreparati nella gestione della minaccia cibernetica, incidendo gravemente nella vulnerabilità dei servizi essenziali. È emersa l'esigenza di rafforzare e integrare le disposizioni della citata direttiva, inglobando gli operatori privati che svolgono attività nei sette settori ritenuti essenziali dall'Unione Europea: energia, trasporti, banche, infrastrutture, mercati finanziari, acqua potabile, sanità e infrastrutture digitali, a cui si affiancano i fornitori di servizi digitali, dall'e-commerce ai motori di ricerca e cloud computing. Il legislatore europeo ha pertanto emanato una ulteriore Direttiva, la 2022/2555/UE, in vigore dal 17 gennaio scorso, denominata **Direttiva NIS 2**, la quale prevede un ulteriore rafforzamento delle misure volte all'implementazione della sicurezza informatica delle reti e dei sistemi informatici dei Paesi membri, ponendosi in prosecuzione degli obiettivi fissati e attuati dalla Direttiva (UE) 2016/1148. La Direttiva (UE) NIS 2 ha portato modifiche in ordine ai soggetti a cui la stessa si applica, ai relativi obblighi, alle sanzioni e all'approccio che deve essere posto in essere nell'adempiere al testo normativo, al fine di giungere all'armonizzazione della disciplina degli Stati membri. Con la Direttiva NIS 2, il legislatore europeo ha implementato i soggetti attivi nei settori definiti *"ad alta criticità"*, includendovi quelli operanti nelle acque reflue, nella gestione dei servizi Ict, della pubblica amministrazione e dello spazio, settori altamente strategici, di impatto pubblico che sono sempre più collegati alle reti digitali al fine di migliorare le reti di trasporto urbano, l'approvvigionamento idrico, gli impianti di smaltimento dei rifiuti, l'efficienza dell'illuminazione e del riscaldamento degli edifici. Tali servizi, sempre più digitali, sono vulnerabili agli attacchi informatici e corrono il rischio, in caso di attacco informatico, di danneggiare i cittadini su larga scala a causa della loro interconnessione, prevedendo anche "altri settori critici", nel quale sono state incluse 12 fattispecie.

L'autorità nazionale per la cybersicurezza

In ambito nazionale, invece, per rispondere adeguatamente alla crescente minaccia cyber, il Governo Draghi, nell'ottica di unificare e potenziare sotto il profilo tecnico operativo, le attività di protezione dalle minacce informatiche, con il Decreto Legge n. 82 del 2021, ha istituito l'**Agenzia per la cybersicurezza nazionale** con una propria autonomia patrimoniale, amministrativa, organizzativa e finanziaria. L'Agenzia, deputata a svolgere il rilevante ruolo di Autorità nazionale di cybersicurezza, ha compiti di protezione, resilienza e innovazione in tema di sicurezza informatica, compresa la tutela della sicurezza nazionale nello spazio cibernetico, assicurando il coordinamento tra i soggetti pubblici coinvolti in materia. L'Agenzia deve promuovere la realizzazione di azioni comuni volte a garantire la sicurezza e la resilienza cibernetica necessarie allo sviluppo digitale del Paese ed è sotto il diretto controllo del Comitato parlamentare per la sicurezza della Repubblica, il quale verifica che l'attività del sistema di informazione per la sicurezza si svolga nel rispetto della Costituzione e delle leggi. Il prefetto **Bruno Frattasi** che è stato chiamato a dirigere

l'Agenzia, dal 9 marzo 2023, ha continuato a dotarla sul piano organico di personale altamente specializzato in frequente crescita, tenuto conto che deve svolgere anche il ruolo di Autorità nazionale di certificazione della cybersicurezza, oltre che Autorità competente in materia di sicurezza di sistemi informatici e alla sicurezza delle reti e Centro nazionale di coordinamento nell'ambito della tutela industriale in materia di cybersicurezza. Nell'ambito dell'Agenzia per la cybersicurezza nazionale opera il **Csirt** *(Computer Security Incident Response Team Italia),* organo essenziale per l'attività tecnico operativa, dato che ha l'obiettivo di migliorare l'efficacia della prevenzione in merito agli attacchi cyber nei confronti di privati o soggetti pubblici, diffondendo informazioni e intervenendo nei casi di emergenza. Mentre, il **Cvcn** *(Centro di Valutazione e Certificazione Nazionale),* che opera sempre all'interno dell'Agenzia, svolge il delicato compito di controllare la sicurezza di beni, sistemi e servizi Ict, adottando delle metodologie che saranno impiegate durante i processi di valutazione del livello di sicurezza, tra cui quello relativo alla predisposizione dell'analisi di rischio. Sempre nell'ambito dell'Agenzia nazionale per la cybersicurezza è istituito il *"Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica",* il quale ha come fine precipuo quello di potenziare la difesa del nostro Paese, con particolare riguardo all'azione di tutela delle infrastrutture critiche del Paese che sono individuate nel sistema delle telecomunicazioni e dei trasporti, l'industria della difesa, gli istituti finanziari, mentre l'**Ncs** *(Nucleo per la cybersicurezza),* ha il compito di rafforzare, sotto il profilo tecnico operativo, la resilienza cyber di tali asset strategici, svolgendo funzioni di prevenzione e preparazione a imminenti situazioni di crisi e per l'attivazione delle procedure di allertamento. L'agenzia, quindi, si pone come punto di riferimento unico della sicurezza cibernetica, con il compito di redigere la strategia nazionale di sicurezza cibernetica e garantire lo svolgimento di azioni comuni per il raggiungimento di più alti livelli di resilienza nazionale, preoccupandosi anche di assumere le funzioni relative al perimetro di sicurezza nazionale cibernetica, operando, infine, come autorità di certificazione della cybersecurity.

Sei indirizzi strategici per la protezione cibernetica

Più in generale, il piano nazionale per la protezione cibernetica e per la sicurezza informatica si compone di sei specifici indirizzi strategici: il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema-paese; il miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati; l'incentivazione della cooperazione tra istituzioni e imprese nazionali; la promozione e la diffusione della cultura della sicurezza cibernetica, il rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica e delle correlate capacità di contrasto alle attività illegali online. Peraltro, i principi cardine estrapolabili dalle politiche di cybersecurity, tanto in ambito internazionale quanto europeo, pongono in evidenza che è indispensabile favorire un approccio comune riguardo le principali questioni strategiche, in completa armonia logica con la globalità di tale dominio. Quindi, focalizzare su tali indirizzi anche il quadro strategico nazionale rappresenta un elemento fondamentale per l'efficienza e la coerenza delle politiche di sicurezza nazionali nel settore. Da queste linee strategiche derivano degli specifici indirizzi operativi da attuare per i prossimi anni, che possono individuarsi: nel potenziamento della capacità di intelligence, di polizia e di difesa civile e militare, nel potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati, nella promozione e diffusione della cultura della sicurezza informatica con periodiche azioni di formazione ed addestramento, nelle iniziative di cooperazione internazionale e nella pianificazione nello sviluppo di esercitazioni finalizzate a testare in concreto l'operatività delle strutture nazionali di prevenzione degli incidenti informatici, procedure di risposta e recupero dei sistemi informatici attaccati.

Tra gli incidenti informatici avvenuti nel 2022 si evidenzia una netta prevalenza di attacchi con finalità di cybercrime Questa tipologia di attacchi, caratterizzata da significativi risvolti economici legati alla diffusione degli attacchi ransomware, mostra una tendenza di crescita costante negli ultimi cinque anni. Anche gli attacchi riconducibili ad attività di spionaggio e sabotaggio (11%), ad information warfare (4%) e ad azioni di attivismo (3%) hanno raggiunto i massimi storici nel 2022. I ricercatori di **Clusit** hanno evidenziato che tra il 2022 e il 2021 gli attacchi compiuti per *"Information Warfare"* sono cresciuti del 110% e quelli di *"Hacktivism"* del 320%. In Italia sono stati il 7% gli incidenti classificati come "attivismo", mentre non sono stati rilevati attacchi significativi nelle categorie *"Espionage/Sabotage"* o *"Information Warfare"*.

Gli enormi profitti illeciti che genera la criminalità informatica vengono spesso reinvestiti dalle organizzazioni nella ricerca di nuove vulnerabilità del sistema e nello sviluppo di capacità offensive più sofisticate, efficienti e di facile utilizzo, rendendo la criminalità informatica una grave minaccia alla stabilità, prosperità e sicurezza di ogni Stato.

Il ruolo degli operatori privati

Se l'approccio strategico all'analisi e alla gestione delle minacce di tale agenzia è il pilastro imprescindibile sul quale costruire anche la tutela dai rischi derivanti dal cyber-spazio, la sicurezza informatica e delle informazioni, non sarà meno importante il ruolo assunto dagli operatori privati, sempre che il loro prezioso contributo si collochi, anche sotto il profilo tecnico e procedurale, nel processo istituzionale volto alla difesa in concreto della sicurezza nazionale e alla gestione delle crisi innescate dai cyber criminali. In particolare. sarà rilevante l'efficace e tempestivo contributo di quegli operatori privati che gestiscono infrastrutture sensibili, il cui funzionamento è condizionato dall'operatività di sistemi informatici, i quali da una parte sono chiamati a comunicare ogni significativa violazione della propria sicurezza o dell'integrità dei propri sistemi informatici al Nucleo per la sicurezza cibernetica e, dall'altra ad adottare le misure di sicurezza predisposte dall'Agenzia per la cybersicurezza nazionale. L'attivismo dei cyber criminali è sempre più organizzato pertanto, a fronte delle evidenze numeriche, gli investimenti nel settore devono essere corposi e assolutamente prioritari, considerando che settori come la PA e Sanità sono pericolosamente esposti alle minacce cyber, come purtroppo abbiamo già avuto evidenti dimostrazioni durante la pandemia con l'attacco al sito della Regione Lazio che ha colpito il sistema informatico sanitario e quello dedicato alla vaccinazione contro il Covid-19. In questo senso, le aziende lasciano comunque trasparire segnali positivi, percependo l'esigenza di crescere per compiere uno switch culturale, dato che nel 2022, per la prima volta, il settore dell'Information Security compare al primo posto nelle priorità di investimento di grandi imprese e Pmi. In tale ambito i fondi del Pnrr possono rivelarsi fondamentali per potenziare il nostro sistema e la collaborazione tra pubblico e privato, completando gli obiettivi comuni di un'azione tesa a incrementare i livelli di sicurezza, affidabilità e resilienza delle reti e dei sistemi informatici, con il rafforzamento della condivisione delle informazioni (anche tra pubblico e privato), l'early warning e le capacità di incident response, compresa l'esigenza aumentare la consapevolezza pubblica della minaccia ed infine incrementare il numero delle figure professionali ad hoc per tutelare il cyber spazio. Un impegno che per ottimizzare la "resilienza digitale" deve necessariamente coinvolgere tutti gli interlocutori del sistema paese, in cui sarà decisivo il ruolo dall'ACN. Quest'ultima ha anche il compito di favorire i percorsi formativi per lo sviluppo di lavoratori del settore e promuovere campagne di sensibilizzazione e diffusione della cultura della cybersicurezza, coinvolgendo nell'applicazione delle misure di prevenzione dei crimini informatici giovani e meno giovani, a prescindere dalle loro abilità informatiche.

Chi è Fabrizio Fratoni

Ufficiale dell'Arma dei Carabinieri in servizio permanente effettivo dal 1992, per aver disimpegnato numerosi incarichi di comando nei reparti dell'Arma **Fabrizio Fratoni** è stato insignito di prestigiosi riconoscimenti, tra cui il Cavalierato dell'Ordine al Merito della Repubblica. Laureato con lode in Giurisprudenza e in Scienze della Sicurezza Interna ed Esterna, è anche abilitato all'esercizio della professione di avvocato. Attualmente è docente di "Sicurezza informatica" nell'ambito del corso di Laurea in Scienze Giuridiche della Facoltà di Economia dell'Universitas Mercatorum di Roma e Criminologo Senior di III Livello certificato da Icmq-Cersa in conformità alla norma UNI 11783:2020.

Le aziende hanno davvero il controllo sui rischi?

Secondo una recente indagine di DNV, nelle aziende manca il senso di urgenza e preoccupazione per la concussione e la corruzione. Poche adottano un approccio strutturato per implementare misure concrete per la gestione dei rischi, mentre la maggior parte si limita ad attuare una politica anticorruzione.

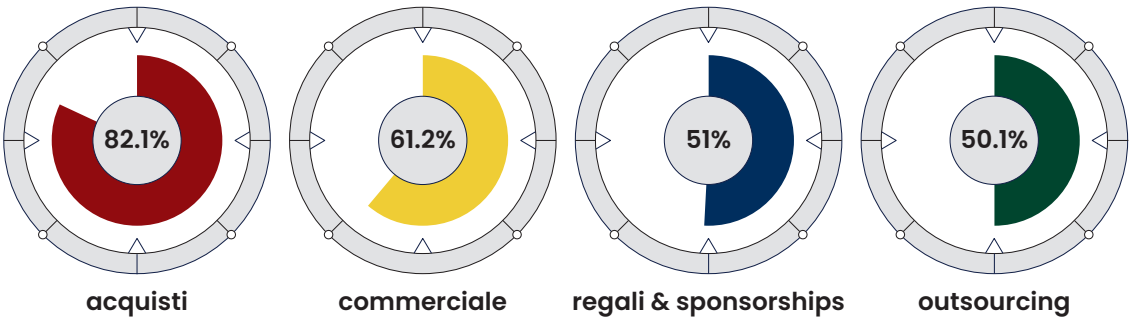
di Cleopatra Gatti

La corruzione preoccupa le aziende, ma sono poche quelle che, per contrastarla, si spingono oltre la sola pubblicazione di una policy anticorruzione. È quanto emerge da un recente studio internazionale condotto da **DNV**, uno dei principali enti di terza parte a livello globale.
L'obiettivo principale per le aziende è la gestione della compliance normativa, della reputazione e dei rischi etici, ma sono limitati, o addirittura nulli, gli investimenti in azioni concrete come, per esempio, la valutazione dei rischi, una due diligence o meccanismi di segnalazione di condotte illecite *(whistleblowing)*. Rimane quindi ancora aperto il tema dell'effettiva conoscenza da parte delle imprese dei rischi in materia di anticorruzione e degli strumenti utili per gestirli.

I costi della corruzione

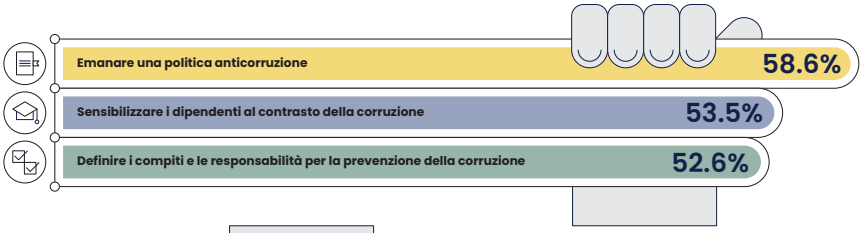
"Il 55% delle aziende coinvolte nello studio ha definito una policy anticorruzione, soltanto il 25% ha stabilito degli obiettivi e appena il 15% ha delineato anche dei Kpi", afferma **Barbara Frencia**, Ceo di Business Assurance in DNV. *"Solo circa un terzo esegue una due diligence sui soci in affari o una valutazione dei rischi. Poche aziende affermano di voler investire di più e questo solleva la questione del grado di implementazione e controllo di cui dispongono le aziende in tema di anticorruzione"*. Si stima che ogni anno, a causa della corruzione, vadano persi in tutto il mondo 2.600 miliardi di dollari, pari al 5% del Pil globale: un forte argomento a sostegno dell'esigenza di approfondire nelle aziende una gestione sempre più proattiva dei rischi, implementando misure volte a prevenire

Aree soggette al rischio di corruzione:



Le aree aziendali più soggette al rischio corruzione
(fonte indagine ViewPoint di DNV)

Le azioni più diffuse mirano a dimostrare l'impegno contro la corruzione:



Le azioni che richiedono maggiori investimenti di tempo e denaro ottengono punteggi più bassi:

L'impegno da parte delle aziende per contrastare il fenomeno della corruzione
(fonte indagine ViewPoint di DNV)

o rilevare tempestivamente le criticità, anziché essere costrette a mitigare i costi di un caso di corruzione.

La mancanza di un approccio preventivo

Lo studio di DNV dimostra che le aziende riconoscono i vantaggi di un sistema di gestione anticorruzione, ma sono poche quelle che adottano un approccio strutturato, finché non sono costrette a farlo a causa di episodi specifici. Solo il 3% afferma di conoscere molto bene la Iso 37001, lo standard per il sistema di gestione anticorruzione: sono 2.896 i certificati rilasciati a oggi, in tutto il mondo, per lo standard Iso 37001. Per confronto, le certificazioni di qualità Iso 9001 rilasciate sono oltre un milione e più di 400mila quelle secondo lo standard ambientale Iso 14001. *"Non conoscere i rischi aziendali sta diventando sempre più costoso. E l'anticorruzione non fa eccezione. Se si considera che la maggior parte degli autori di frodi ha già mostrato comportamenti sospetti in precedenza e che la maggior parte delle aziende vittime modifica i propri controlli dopo un incidente, è evidente che implementare un approccio preventivo e strutturato sotto forma di un sistema di gestione conforme alla norma ISO 37001 è essenziale"*, conclude Barbara Francia. Le aziende che adottano un approccio anticorruzione basato sullo standard Iso 37001, riconosciuto a livello internazionale, sono più attive nell'intraprendere un percorso di mappatura dei rischi, assicurandosi di essere meglio attrezzate per gestirli e prevenirli, anziché mitigarli. Il 61% delle imprese che dispongono di una policy ha stabilito anche dei Kpi, il 64% esegue una valutazione dei rischi e il 57% effettua una due diligence sui soci in affari. Il 43% prevede inoltre una funzione anticorruzione dedicata, che contribuisce a prevenire il potenziale conflitto di interessi che può verificarsi quando la responsabilità è attribuita a un amministratore delegato o top manager responsabile anche delle attività operative e del conto economico.

La maggior parte delle aziende non basa il proprio approccio sulle buone pratiche standard né implementa un sistema di gestione anticorruzione. Sebbene i rischi corruttivi siano molto concreti, all'apparenza le potenziali minacce non sono una priorità nelle aziende. L'atteggiamento prevalente sembra essere *"da noi non può succedere"*. È possibile che la lotta alla corruzione stia perdendo priorità nei piani aziendali a causa di criticità più recenti, come la pandemia e i conflitti internazionali, che rendono più prioritarie la sicurezza, l'energia e la sicurezza informatica.

Barbara Frenzia, Ceo in Business Assurance, **DNV** (Crediti: **Marco Pesenti**)

La corruzione, una piaga insidiosa

Nella sua prefazione al testo della Convenzione delle Nazioni Unite Contro la Corruzione del 2004, l'allora Segretario Generale Onu **Kofi Annan** descrisse la corruzione come *"una piaga insidiosa che produce una vasta gamma di effetti corrosivi sulle società. Mina la democrazia e lo stato di diritto, porta a violazioni dei diritti umani, distorce il mercato, erode la qualità della vita e consente di prosperare alla criminalità organizzata, al terrorismo e ad altre minacce alla sicurezza umana"*. A più di dieci anni di distanza da queste parole di Kofi Annan, in occasione della Giornata internazionale contro la corruzione del dicembre 2018, il Segretario Generale delle Nazioni Unite **António Guterres** ha stimato i costi annuali della corruzione internazionale nell'incredibile cifra di 3.600 miliardi di dollari in tangenti o denaro sottratto.

La corruzione può assumere molte forme: tangenti, appropriazione indebita, riciclaggio, evasione fiscale e clientelismo, solo per citarne alcune. Per molte aziende, il rischio maggiore sono le tangenti, cioè l'azione di un singolo individuo che, per ottenere un contratto più remunerativo per il proprio datore di lavoro o superiore, offre denaro a un dipendente corrotto di un'altra società, un funzionario governativo o anche un politico di alto rango.
In alcuni casi, la corruzione si protrae per lunghi periodi e può aumentare gradualmente da piccoli regali personali a ingenti somme di denaro, nell'ordine anche dei miliardi di dollari. Indipendentemente dalle sue dimensioni o reputazione, non ne è immune nessuna azienda, come dimostra chiaramente il numero di cause e processi che coinvolgono ogni anno le multinazionali.

Peggiora la percezione della nostra sicurezza

Diminuiscono le persone che si sentono sicure nella propria città e riprendono i reati predatori, soprattutto le rapine. In lieve aumento gli omicidi: quelli delle donne vengono compiuti in ambito familiare e di coppia.

di Laura Reggiani

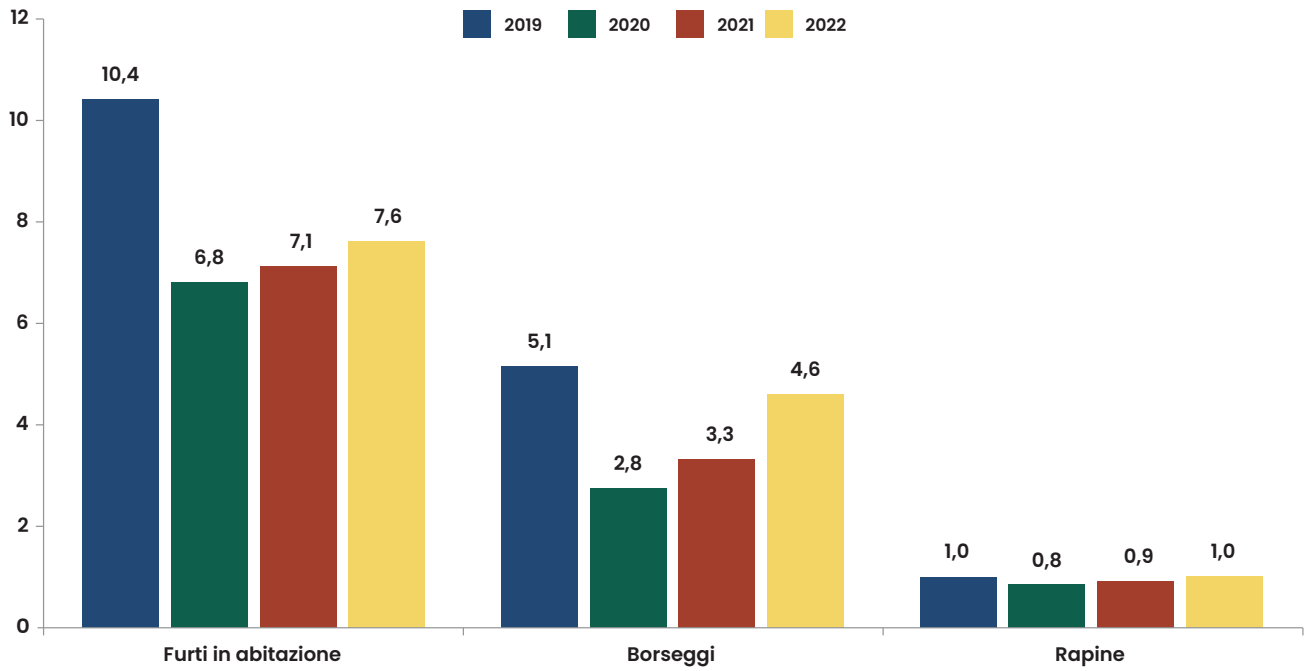
Gli omicidi e i reati che nel primo anno di pandemia avevano toccato i valori più bassi di tutta la serie storica, nel 2021 sono tornati a registrare una lieve crescita e per i reati predatori l'incremento è proseguito anche nel 2022. Gli indicatori soggettivi di percezione si sono mossi nello stesso modo degli indicatori oggettivi relativi ai reati: nel 2022, gli indicatori di percezione di sicurezza hanno infatti interrotto il trend positivo registrato nei due anni di pandemia: è diminuita la percezione di sicurezza e aumentata la percezione del rischio di criminalità, mentre è rimasta stabile la percezione del degrado. Sono questi i dati più significativi che emergono dall'ultimo *"Rapporto sul Benessere equo e sostenibile"* pubblicato da **Istat** nel 2023, che ha registrato l'impatto sul Paese degli ultimi tre drammatici anni, dominati dalla pandemia, dalle crisi ambientali, e dallo scoppio della guerra in Ucraina.

Meno sicurezza percepita

Nel 2022 la quota di persone che si dichiarano molto o abbastanza sicure quando camminano al buio da sole nella zona in cui vivono diminuisce di 1,6 punti percentuali, attestandosi al 60,6% (era il 62,2% nel 2021 e il 57,7% nel 2019) e aumenta di 1,3 punti la quota di famiglie che affermano che la zona in cui vivono è molto o abbastanza a rischio di criminalità, arrivando al 21,9% (era il 20,6% nel 2021, il 25,6% nel 2019). Rimane stabile al 6,9% la quota di popolazione che dichiara di aver visto nella zona in cui abita persone che si drogano o spacciano droga, prostitute in cerca di clienti o atti di vandalismo contro il bene pubblico (6,3% nel 2021, l'8,3% nel 2019). Si sentono più sicure, percepiscono un minor rischio di criminalità e un minor degrado sociale e ambientale le persone residenti nei comuni fino a 2mila abitanti e in quelli tra 2mila e 10mila abitanti, rispetto a quelle residenti nei comuni di grandi dimensioni. Nei comuni tra 2mila e 10mila abitanti la quota di persone di 14 anni e più che si dichiarano molto o abbastanza sicure quando camminano al buio da sole nella zona in cui vivono è 17 punti più alta rispetto a quella riscontrata nei comuni centro delle aree di grande urbanizzazione e analogamente succede per la percezione del rischio di criminalità e per il degrado sociale e ambientale. La percezione di sicurezza varia secondo il genere, l'età e il titolo di studio. Il 70,9% degli uomini si sentono sicuri contro poco più della metà delle donne. La situazione è diversa anche in relazione alle età: i più insicuri sono gli anziani di 75 anni e più, mentre i giovani e gli adulti percepiscono un maggiore livello di sicurezza.

La ripresa dei reati predatori

Nel primo anno della pandemia, le misure restrittive alla mobilità e ai contatti sociali avevano portato a una forte riduzione dei reati predatori, ovvero furti in abitazione, borseggi e rapine. Questi reati hanno toccato nel 2020 i valori più bassi dopo il picco toccato nel 2013/2014. Poi



L'andamento di furti in abitazione, rapine e borseggi negli ultimi 4 anni
(dati ogni 1000 abitanti, fonte Rapporto BES - Istat 2023)

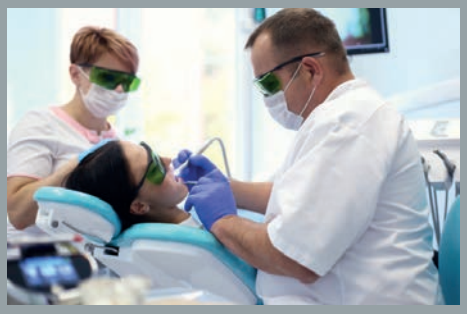
dal 2021, con l'allentamento delle misure restrittive e il ritorno alla normalità questi reati hanno iniziato a registrare una lieve crescita, proseguita anche nel 2022. I tassi dei furti in abitazione e i borseggi sono rimasti al di sotto dei valori pre-pandemia, mentre il tasso di rapine è tornato sui livelli del 2019. Nel 2022 il tasso di vittime di furti in abitazione si attesta al 7,6 per 1.000 famiglie (rispetto al 7,1 del 2021 e al 10,4 del 2019), il tasso di vittime di borseggi ammonta a 4,6 vittime ogni 1.000 abitanti (rispetto al 3,3 del 2021, 5,1 nel 2019) e quello delle vittime di rapine a 1 vittima ogni 1.000 abitanti (era pari allo 0,9 nel 2021 e all'1,0 nel 2019). I reati predatori si distribuiscono in modo diverso sul territorio con una maggiore concentrazione nelle regioni del Centro-Nord rispetto a quelle del Mezzogiorno. Nel 2022, il tasso più alto di vittime di borseggi si riscontra nel Centro e nel Nord-Ovest. I furti in abitazione sono più diffusi nel Centro-Nord e in particolare nel Nord-Est. Per le rapine, invece, le differenze sono più contenute. Nel 2022 le vittime di furti in abitazione ogni 1.000 famiglie e le vittime di borseggio ogni 1.000 persone aumentano in tutte le ripartizioni geografiche, ma in modo più accentuato nel Nord-Ovest e nel Centro. Per quanto riguarda le vittime di rapine il tasso rimane stabile nel Nord-Est, mentre aumenta in tutte le altre aree geografiche. I tassi dei furti in abitazione rimangono inferiori a quelli del 2019, mentre per i borseggi solo il Nord-Ovest è tornato sui livelli del 2019. Più articolata la situazione per le rapine: rispetto alle quali il Nord ha superato i livelli prepandemici, il Centro si colloca sullo stesso livello, mentre nel Mezzogiorno i tassi rimangono inferiori a quelli registrati prima della pandemia.

Aumentano gli omicidi, donne vittime in ambito familiare

Nel 2021, in Italia sono stati commessi 308 omicidi, lo 0,52 per 100mila abitanti, un tasso in lieve aumento rispetto al 2020 quando si attestava a 0,49 per 100mila abitanti (per un totale di 289 omicidi). Nonostante nel lungo periodo la diminuzione del tasso di omicidi più consistente si osservi nel Mezzogiorno, questa area continua a registrare il tasso più alto. In Italia la dimensione quantitativa degli omicidi è molto contenuta se paragonata a quella degli altri Paesi, posizionandosi penultima in graduatoria (0,48 omicidi per 100mila abitanti nel 2020), dopo il Lussemburgo. Nel 2021, le vittime di omicidio sono state 183 uomini e 125 donne. Sebbene il tasso di omicidi degli uomini sia maggiore rispetto a quello delle donne, è da considerare che per le donne la diminuzione ha seguito ritmi molto più lenti ed è riconducibile a una riduzione del numero di vittime da autore sconosciuto, piuttosto che a un calo delle vittime in ambito familiare. Se si esamina la relazione tra autore e vittima dell'omicidio, si nota che le donne sono uccise soprattutto nella coppia e in ambito familiare, gli uomini sono invece vittime di un autore sconosciuto. Nel 2021, l'89,1% degli omicidi femminili risulta compiuto da una persona conosciuta. In particolare, nel 2021, circa 6 donne su 10 sono state uccise dal partner attuale o precedente, il 25,2% da un familiare e il 5% da un'altra persona che la donna conosceva. Stuazione diversa per gli uomini: nel 2021 solo il 36,4% è stato ucciso da una persona conosciuta e solo il 4,3% da un partner o ex partner. Nel 63,6% dei casi a uccidere è stato uno sconosciuto o autore non identificato.

Il “giusto” equilibrio tra lavoro e famiglia

Gruppo RTS, attraverso l'adesione a EBITEN, supporta i piani di Welfare Aziendale che sostengono il lavoratore e la sua famiglia aumentando la competitività aziendale



Salute e sicurezza, servizi per la famiglia, rimborso spese di istruzione, sconti su beni e servizi sono alcuni degli esempi dei vantaggi disponibili per i dipendenti delle aziende iscritte ad Ebiten.

GRUPPO rts REAL TRAINING SOLUTIONS

Ente Bilaterale Nazionale del Terziario EBITEN

Contattaci per avere maggiori informazioni sui piani di Welfare Aziendale

www.rts-srl.it **800 010 333** **info@rts-srl.it**

A CURA DI GIORGIA ANDREI

Professionalizzare le risorse umane e costruire competenze strategiche

Il Fondo Interprofessionale **Formazienda** ha emanato l'avviso di finanziamento 2/2022 stanziando 25 milioni di euro con lo scopo di riqualificare la forza lavoro per consentire al sistema imprenditoriale di generare ricchezza, posti di lavoro e innovazione. La strategia di Formazienda, il Fondo interprofessionale per la formazione continua, istituito da **Confsal** e **Sistema Impresa**, è in linea con i traguardi di rinnovamento indicati dal Piano nazionale di ripresa e resilienza che ha visto gli esecutivi nazionali collaborare con la Commissione UE per costruire una prospettiva di ritorno alla crescita. *"La formazione continua"* dichiara il direttore generale **Rossella Spada** *"può esercitare un ruolo fondamentale per ricondurre l'economia italiana a uno stato di salute e prosperità. Il sistema Paese ha una forza imprenditoriale dotata di grandi potenzialità. L'avviso di finanziamento 2/2022 è stato incrementato per dare seguito ai talenti delle aziende e perché le sfide del Pnrr sono ambiziose. Le imprese devono essere messe nelle condizioni di affrontare mercati ostici dove qualificare e riqualificare le risorse umane è una priorità. In merito alle tematiche dei piani formativi, queste interessano naturalmente gli ambiti strategici. Occorre il massimo livello di efficienza e di efficacia in relazione agli obiettivi della trasformazione tecnologica ed ecologica, dell'internazionalizzazione e della sicurezza"*.

PERCORSI FORMATIVI

Un futuro in divisa

Circa il 6% degli studenti in uscita dalle scuole superiori si dichiarano fortemente interessati a una carriera nell'ambito delle Forze Armate e di Polizia e la pongono come prima opzione su cui puntare per costruire il proprio futuro. L'annuale **Osservatorio sulle Professioni in divisa 2022**, realizzato da **Skuola.net** in collaborazione con **Nissolino Corsi**, ha messo in luce l'identikit dell'aspirante *"divisa"*, sfatando parecchi luoghi comuni. Tra chi mostra un interesse verso le carriere in divisa, oltre 4 su 10 dichiarano un rendimento negli studi di tutto rispetto e solo uno su 5 ammette pagelle con molte insufficienze. Il contesto sociale di provenienza smentisce un pregiudizio diffuso: oltre 4 su 10 ritengono di avere una situazione economica *"tranquilla"*, il 31% dice di appartenere a una famiglia *"mediamente agiata"* e l'11% di essere *"molto agiato"*. Qualcosa di simile avviene per il livello di istruzione del contesto di provenienza: il 19% considera i genitori *"altamente istruiti"*, il 33% *"mediamente istruiti"*. Per restare in famiglia, tra chi si dichiara disposto a entrare nelle Forze Armate o di Polizia, due su tre hanno almeno un membro della propria famiglia (genitori, fratelli, nonni, zii ecc.) che indossa o ha indossato in passato una divisa.

CORSI AICIS

Due corsi per criminologi e non solo

Segnaliamo due corsi utili fruibili dalla piattaforma di e-learning **Zero Academy Criminology Intelligence Security**. Il primo è ***"Analisi emotivo comportamentale e valutazione della credibilità dell'interlocutore",*** della durata di 5 ore, che vale 5 crediti formativi per criminologi certificati UNI11783 e professionisti della security secondo la normativa UNI10459. Consente di acquisire le competenze per valutare la credibilità dell'interlocutore e indagare gli indizi di menzogna: microespressioni del volto, piccoli gesti delle mani, movimenti del corpo, velocità dell'eloquio ecc. Il secondo si intitola ***"Esperto di sopralluogo e fotografia giudiziaria e investigativa"*** e vale anche in questo caso 5 crediti per Criminologi UNI 11783, Security Manager Certificati e Periti Liquidatori Assicurativi UNI 11628. Il corso tratta tematiche legate alle tecniche del sopralluogo e alla tecnica della documentazione fotografica e video, incluso l'utilizzo della luce nella foto giudiziaria. Maggiori informazioni sul sito di **Aicis**.

CORSI FEDERPOL

Restare sempre aggiornati con Federpol

I corsi di aggiornamento organizzati da **Federpol** sono validi per le istanze di rinnovo delle autorizzazioni ai sensi del D.M. 269/2010 e, ai sensi del regolamento sulla Formazione continua approvato dal Consiglio Nazionale Forense, sono stati riconosciuti ai corsi 5 crediti formativi. Direttore dei corsi è il professor **Roberto Mugavero**, presidente di **Osdife CBRNe**. Per l'autunno, ecco le date in programma:

22 settembre - Verona
06 ottobre - Bologna
20 ottobre - Bari
17 novembre - Firenze
01 dicembre - Roma

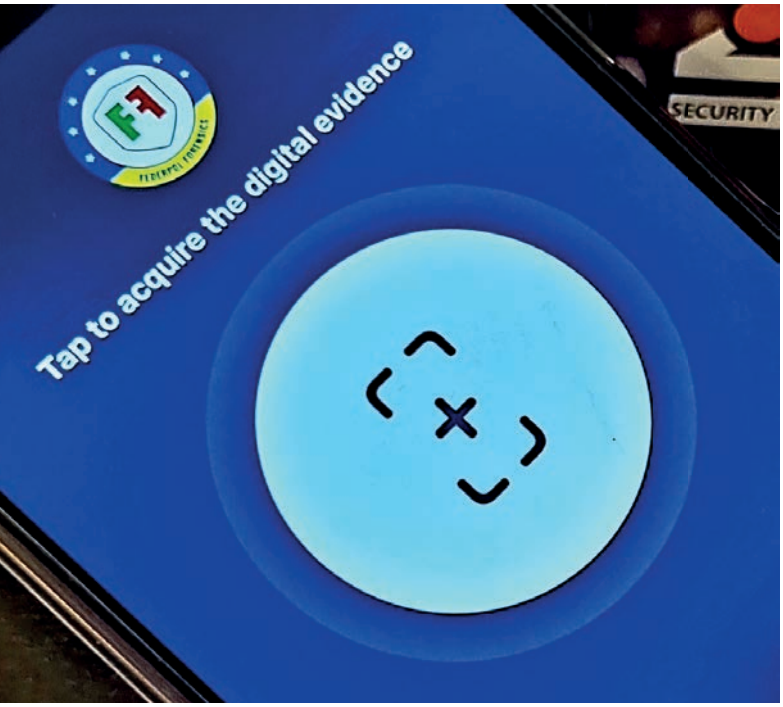
DI BARIĆ ROKO*

Federpol Forensics: un approccio moderno all'acquisizione di prove digitali

In collaborazione con **TrueScreen**, **Federpol** ha sviluppato l'applicazione mobile **Federpol Forensics**, strumento di lavoro destinato agli investigatori privati per l'acquisizione forense di prove digitali (foto, video, audio, localizzazione, screenshot ecc.) direttamente da dispositivi mobili. L'applicazione crea un ambiente forense all'interno dello smartphone e poi certifica le prove, impedendo così modifiche al contenuto stesso. Questo modo di escludere le prove è coerentemente conforme allo standard Iso/Iec 27037:2012, alle linee guida eIDAS e Gdpr. Inoltre, il metodo dell'esenzione è riconosciuto dal governo italiano, seguendo le linee guida emanate dal Consiglio d'Europa nella convenzione "Cybercrime" e dai tribunali italiani. L'investigatore privato, al momento di finalizzare la denuncia delle prove, appone sul documento la sua firma digitale avanzata, che conferma la correttezza e la professionalità nel processo di assunzione delle prove. L'applicazione estrae i dati dei metadati dai materiali raccolti e protegge il contenuto da eventuali manipolazioni. Chiedersi dove, quando, come e con cosa il materiale o le prove sono stati esclusi e se sono stati manipolati diventa quasi impossibile. Il rapporto e i materiali prodotti rimangono collegati e facilmente confrontabili.

Finalità e vantaggi della app

L'applicazione ha diversi scopi, ma i due che ci interessano di più e che attualmente sono conformi alla legge sugli investigatori privati, sono la registrazione dello schermo e la cattura di foto. Quando parliamo dell'opzione di registrazione dello schermo, pensiamo innanzitutto ai messaggi provenienti da dispositivi mobili. Finora gli investigatori hanno utilizzato diversi metodi per estrarre tali messaggi, con vantaggi e svantaggi. L'applicazione Federpol Forensics permette di registrare in tempo reale il contenuto di una conversazione scritta, indipendentemente dal software utilizzato per lo scambio di comunicazioni. Nel report finale, oltre alla visualizzazione delle immagini dei messaggi, abbiamo informazioni complete su quando sono stati scaricati e da quale dispositivo e protezione che non siano stati successivamente manipolati. Ci vogliono solo pochi minuti per farlo: si accede all'applicazione e si attiva la registrazione dello schermo, registrando il contenuto della comunicazione. Successivamente viene redatto un verbale, al quale l'investigatore appone la sua firma e la procedura è conclusa. La cattura della foto tramite l'applicazione, insieme a molti vantaggi in termini di sicurezza, consente di registrare il luogo in cui è stata scattata la foto. Pertanto, è necessario scattare meno foto dell'oggetto dell'indagine. La pratica precedente di scattare foto da più angolazioni per dimostrare la posizione diventa superflua. Quando si scattano foto di oggetti danneggiati o ritrovati, è molto importante avere una registrazione trasparente del luogo e dell'ora in cui è stata scattata la foto. Ciò è particolarmente evidente nelle investigazioni legate a frodi assicurative, danni alla proprietà del cliente e altre tipologie di investigazioni con epilogo potenzialmente giudiziario. Per quanto riguarda la registrazione video, dopo avere realizzato la ripresa l'utente seleziona le clip essenziali destinate al report finale. La denuncia è così corredata da un video completo e dotata di firma digitale avanzata. Su questi clip e video, come su altre prove digitali esentate tramite l'applicazione, sono stampati tutti i metadati e si ottiene la protezione da qualsiasi forma di manipolazione. Non è quindi possibile modificare o falsificare firme, date e altre parti importanti a seconda dei documenti necessari nelle indagini.



A chi può essere utile Federpol Forensics?

Oltre all'utilizzo negli ambienti degli investigatori, l'applicazione ha prospettive di utilizzo anche per compagnie di assicurazione e periti, in caso di incidenti stradali, sicurezza sul lavoro ecc. Anche se l'applicazione e i dispositivi mobili non sono ancora al livello di poter sostituire completamente l'attrezzatura fotografica professionale, si tratta comunque di un progresso significativo.

* **Barić Roko**, investigatore privato e segretario di **HRPD Hrvatski Red Provatnih Detekti.**

A CURA DI GIORGIA ANDREI

Più protetti con la copertura assicurativa Das

L'accordo stipulato da **Federpol** con **Das Tutela Legale** prevede per gli associati una copertura assicurativa per le spese legali, peritali e processuali derivanti da eventuali procedimenti penali. Corrispondendo la propria quota, quindi, il socio usufruisce di un servizio di grande valore. Das è parte di **Generali Italia** e **Gruppo Ergo** (Munich Re), ha sede a Verona e opera con oltre 1.500 intermediari su tutto il territorio nazionale, che offre consulenza legale telefonica immediata, assistenza legale e peritale in tutta Europa. Con la tutela legale, Das assume a proprio carico, nei limiti delle condizioni e del massimale stabiliti dalla polizza, il rischio dell'assistenza giudiziale che si renda necessaria a tutela degli assicurati in conseguenza di un caso assicurativo rientrante in garanzia. La copertura è valida sia nel caso di procedimento penale colposo sia nel caso di procedimento doloso.

Nel secondo caso la tutela si sostanzia nella difesa legale, purché l'assicurato sia prosciolto o assolto con decisione passata in giudicato: è in questo momento che Das rimborserà le spese sostenute. Va sottolineato che, sempre nell'ambito del procedimento doloso, la garanzia è operante anche nell'ipotesi in cui sia intervenuta: la derubricazione del reato da doloso a colposo; l'archiviazione per infondatezza della notizia di reato; la prescrizione del reato. La polizza include la tutela legale anche nel caso in cui all'assicurato siano notificate contravvenzioni per violazione della privacy, un aspetto molto delicato nell'operatività dell'investigatore privato. Da segnalare che Das mette a disposizione un numero verde al quale accedere, in modo illimitato, per chiedere consulto a un avvocato, anche su temi normativi dei quali si voglia comprendere l'impatto sulla propria attività.

SERVIZI

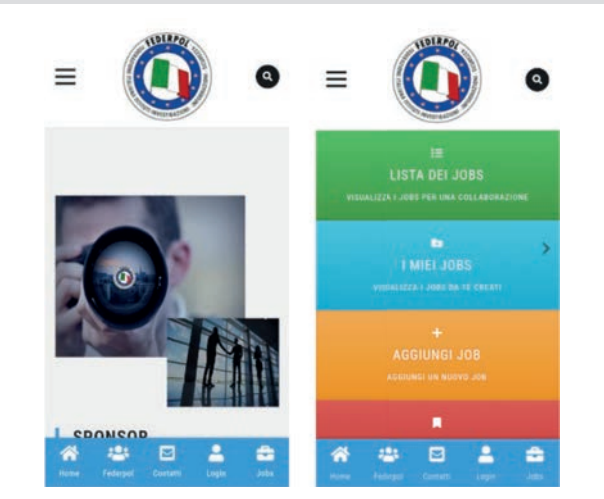
Sicurezza, welfare, contrattualistica: Ebiten c'è

Ebiten è l'organismo bilaterale individuato nel Contratto nazionale dei lavoratori per il settore delle investigazioni private e della sicurezza complementare sottoscritto da **Federpol** insieme a **Sistema Impresa**, **Confsal** e **Fesica Confsal**, enti dai quali Ebiten stesso è nato nel 2009. Direttamente o in partenariato con Federpol, Ebiten eroga diversi servizi a favore delle agenzie investigative che applicano il Ccnl di riferimento. Le prestazioni interessano, oltre alla formazione, gli ambiti della sicurezza e salute sul lavoro, del welfare e della contrattualistica. Segnaliamo in particolare che si possono richiedere a Ebiten: pareri di conformità sulla formazione individuale per l'assunzione di apprendisti, servizi di intermediazione tra domanda e offerta di lavoro, assistenza contrattuale sull'applicazione del Ccnl.

APP

Federpol App: mai più senza

Scaricando (da Apple Store o Google Play Store) e installando **Federpol App** è possibile ricevere notifiche sulle ultime pubblicazioni di interesse per gli investigatori privati e non solo: la App, infatti, è anche uno strumento utile per creare rapporti di collaborazione tra i membri dell'associazione attraverso la sezione **"Jobs"**. Ecco come funziona: una volta scaricata l'app, occorre eseguire il login tramite l'apposito pulsante di accesso all'area riservata e cliccare sulla voce Jobs. Da qui è possibile avanzare richieste di collaborazione ad altri soci Federpol compilando una serie di campi nella sezione **"Aggiungi Job"** e contattare altri soci titolari che hanno scaricato l'app per iniziare rapporti di collaborazione con gli stessi.



A CURA DI CLEOPATRA GATTI

Sicurezza: più denunce a Milano, Rimini e Bologna

È stata pubblicata da **Il Sole24Ore** la lista delle città più pericolose d'Italia che si basa su dati statistici che provengono dal Dipartimento di **Pubblica Sicurezza del Ministero dell'Interno** in merito ai reati per i quali è stata sporta denuncia nel 2022. Nelle prime posizioni figurano i nomi di grandi città, che non solo vedono la presenza di milioni di abitanti, ma che rappresentano il fulcro del turismo nazionale sempre più numeroso. Questi dati, quindi, fanno emergere in modo chiaro come ci sia una connessione tra atti criminali e presenza massiccia di turisti. Milano detiene il primo posto di questa classifica delle città più pericolose d'Italia. È proprio nel capoluogo lombardo, infatti, che si verificano il maggior numero di reati e azioni criminali da parte di bande organizzate. Soltanto lo scorso anno, sono state più di 8.500 le denunce per reati ogni 100mila abitanti. La maggior parte di questi atti riguardavano rapine all'interno di edifici o furti di auto parcheggiate. Per quanto riguarda il numero totale degli omicidi, questi sono in calo rispetto ai dati di riferimento che abbiamo dagli anni precedenti. Nonostante siano stati molto elevati, i furti e le rapine sono diminuiti. Un dato preoccupante e in crescita è quello che riguarda le truffe informatiche che si verificano nel territorio milanese. Collegati a quest'ultimo ambito sono i reati legati alla pedo-pornografia e lo stalking in rete. In più, sono sempre maggiori i casi di frode tramite falsificazione di carte di credito e di denaro contante. Ma da cosa dipende questo triste primato di Milano? Principalmente, i numeri relativi ai reati sono connessi anche a una maggiore tendenza dei cittadini milanesi a sporgere denuncia rispetto ad altre zone del nostro Paese. In più, a incidere in modo rilevante sono i casi di borseggi nelle stazioni, nella metropolitana e nei pressi dei monumenti più importanti, oltre che i furti nei negozi, in relazione anche al tenore di vita abbastanza elevato. Al secondo posto troviamo la città di Rimini. In questo caso, per il 2022, le denunce sono state circa 8mila per ogni 100mila abitanti. Questi dati, se rapportati alla popolazione totale, sono allarmanti. Oltre ai casi di borseggi, che stanno crescendo, aumentano anche i furti negli appartamenti, eventi che stanno preoccupando sempre di più gli abitanti del luogo e i turisti. Alto è il numero delle violenze sessuali, per le quali Rimini si pone al primo posto in Italia, con una, seppure leggera, crescita di anno in anno. Tra i reati maggiori troviamo anche l'evasione fiscale che cresce parallelamente alla crisi economica ed è in netto peggioramento. Sul gradino più basso del podio ancora una città dell'Emilia-Romagna. Le denunce nel 2022 a Bologna sono state poco più di 7mila per ogni 100mila abitanti. Tra i reati più frequenti ci sono rapine e truffe. Ad aumentare sono anche gli scippi che hanno registrato il picco più alto degli ultimi dieci anni. Unico trend in calo, per fortuna, sono gli omicidi. Appena dietro Bologna, al quarto posto, troviamo la città di Torino. Secondo la classifica, sono 7mila le denunce per ogni 100mila abitanti del capoluogo piemontese. Tra i reati più comuni abbiamo furti, borseggi e atti di danneggiamento a negozi e veicoli. Confortante il dato sugli omicidi, mentre è in crescita quello relativo a violenze, minacce e lesioni.

Roma chiude con circa 6.600 denunce per ogni 100mila abitanti che riguardano, principalmente, furti e violenze. A essere maggiormente colpiti, com'era immaginabile, sono stati i turisti che ogni anno affollano il centro storico e i mezzi di trasporto della città eterna. In diminuzione, invece, i reati ancora più violenti come violenze sessuali e omicidi.

IL REPORT

I numeri delle persone scomparse

Il Report realizzato dal Commissario straordinario Prefetto **Maria Luisa Pellizzari** descrive l'andamento del fenomeno relativo alle persone scomparse in Italia, avendo cura di riportare i dati relativi al primo semestre 2023 comparati con il primo semestre dell'anno precedente. I dati, messi a disposizione dal **Dipartimento della Pubblica Sicurezza – Direzione Centrale della Polizia Criminale**, consentono un monitoraggio generale a partire dal 1° gennaio 1974 al 30 giugno 2023, con un totale di 235.999 ritrovamenti (pari al 72,8%) su un complessivo di 324.389 denunce di scomparsa registrate dalle Forze di Polizia. Alla data del 30 giugno 2023, le denunce di scomparsa attive sono 88.390. Nel periodo di riferimento (1° gennaio

– 30 giugno 2023), i dati registrati sul fenomeno contano 6.297 ritrovamenti su un totale di 13.031 denunce di scomparsa, con 6.734 denunce attive. In questo range temporale, mettendo in relazione il totale delle 13.031 denunce con il numero degli scomparsi distinti per fascia di età, si conferma che il 73,9% (9.626 casi) attiene alla fascia under 18, il 22,5% (2.934 casi) corrisponde alla fascia della maggiore età e il 3,6% (471 casi) appartiene alla fascia di età degli over 65. I dati sulle persone scomparse di nazionalità italiana indicano che nel primo semestre 2023 sono state ritrovate 3.419 persone, pari al 75,5% del totale delle denunce di scomparsa (4.531). Restano pendenti 1.112 casi (24,5%).

A CURA DI CLEOPATRA GATTI

Dalla Biblioteca Federpol, letture per i professionisti delle investigazioni

Sono diversi i volumi stampati col patrocinio di **Federpol** negli ultimi anni, in diverse aree di interesse per i professionisti delle investigazioni e della sicurezza.

In ambito assicurativo, il volume di riferimento è **"Frode assicurativa e reati connessi"**, edito da **Giappichelli Editore** e scritto da **Mario Riccardo Oliviero** e **Federica Sulis**. Le frodi assicurative rappresentano un fenomeno, che, però, non è sempre accompagnato da una piena conoscenza delle fattispecie penali interessate. In un quadro spesso incerto e molto articolato, diventa indispensabile ordinare e approfondire le caratteristiche e le implicazioni connesse a questi reati attraverso un compendio di diritto assicurativo penale. Con queste premesse il libro intende fornire un adeguato supporto tecnico non solo agli operatori giuridici e assicurativi, ma anche a tutti coloro che abbiano interesse ad approfondire il tema.

A chi vuole affrontare il tema della privacy consigliamo **"Il trattamento dei dati personali nell'attività investigativa"**, uno scritto a cura dell'avvocato **Marco Martorana** e di **Luciano Tommaso Ponzi**. L'opera nasce per fornire indicazioni teoriche e operative sul trattamento dei dati personali a chi svolge attività di tipo investigativo, per consentire di trovare il necessario bilanciamento tra la privacy degli individui e lo svolgimento delle investigazioni. Vengono affrontati gli argomenti di base per la tutela dei dati, con specifici riferimenti al contesto investigativo e delle informazioni commerciali, per poi approfondire la trattazione con focus sulla sicurezza informatica, sulle nuove tecniche di raccolta delle informazioni come l'Osint e sull'Attività ispettiva del Garante per la protezione dei dati personali.

Per quanto riguarda l'ambito della Tutela Marchi, **Francesco Sardi de Letto** e **Luigi Levori** propongono il loro libro **"La tutela giuridica del marchio"**, edito da **Key Editore**. L'opera è stata concepita con l'obiettivo di fornire una guida pratica ma, per quanto possibile, completa sulla tutela del marchio. Viene passata in rassegna la funzione del marchio nel campo giuridico commerciale e le varie tipologie dei segni distintivi, con particolare riferimento ai marchi di qualità. Sono state riassunte le fonti normative ed è stato dato particolare risalto alla tutela giuridica assegnata. Infine, è stato analizzato l'istituto della concessione di vendita e della vendita selettiva, precisando il concetto del principio di esaurimento del marchio.

ROMANZO GIALLO

Gatti neri in libreria

Piergiorgio Pulixi firma un giallo pieno di suspense e ironia che parla di libri e omaggia i classici del mystery. **"La libreria dei gatti neri"** racconta di Marzio Montecristo, proprietario una piccola libreria specializzata in romanzi gialli nel centro di Cagliari. Il nome della libreria è un omaggio ai due gatti neri presenti in negozio Miss Marple e Poirot. La libreria ha anche un gruppo di lettura, *"gli investigatori del martedì"*, super esperti di gialli che si riuniscono dopo la chiusura per discutere del romanzo della settimana. La sovrintendente Angela Dimase chiede la loro collaborazione per un'indagine su una serie di fatti tremendi che le sta togliendo il sonno. Riusciranno gli improbabili *"investigatori del martedì"* a sbrogliare anche questo caso, intricato quanto agghiacciante, permettendo alla polizia di fermare il feroce assassino prima che colpisca di nuovo?

SAGGIO CRIMINOLOGIA

Storie di efferati assassini

Perché l'ha fatto? Ce lo chiediamo davanti a delitti feroci. L'istinto ci porta a credere che il male sia frutto della follia o di un raptus omicida. Ma la verità e che esistono persone malvagie e che ogni azione violenta è sempre la conseguenza di ciò che è andato costruendosi nel tempo. Ce lo dimostra **Stefano Nazzi** ne **"Il volto del male"**, una raccolta di storie inquietanti. Con una prosa coinvolgente, racconta le vicende di dieci persone che hanno fatto il male e ben lo rappresentano: uomini e donne di età diverse, che in Italia si sono resi colpevoli di delitti efferati, spesso con moventi inesistenti. Dai più noti, come Nicola Sapone delle Bestie di Satana o Luigi Chiatti, il Mostro di Foligno, a nomi meno conosciuti.

ROMANZO GIALLO

Impedire un omicidio già avvenuto

È mezzanotte nei sobborghi di Liverpool. Jen, affacciata alla finestra, sta aspettando che il figlio diciottenne torni a casa. Ecco che il ragazzo compare, ma in pochi secondi Jen assiste a una scena che non si sarebbe mai immaginata: suo figlio Todd accoltella un uomo sconosciuto. Non sa chi sia. Non sa perché. Sa solo che il suo futuro è distrutto. Diverse ore più tardi, si addormenta stremata. Ma quando si sveglia è il giorno precedente. La scena da incubo a cui ha assistito non ha ancora avuto luogo. Questo viaggio a ritroso nel tempo comincia a ripetersi a ogni risveglio: è l'occasione, per Jen, di ripercorrere la loro vita familiare alla ricerca di indizi. Da qualche parte, nascosta nel passato, c'è una soluzione e Jen deve trovarla. **Gillian McAllister** firma il thriller dell'anno **"Posto sbagliato momento sbagliato"**, un avvincente mistero che si svela in un crescendo di tensione costruito in maniera magistrale.

Scrivere a *mag@federpol.it*

Buongiorno, sono titolare di una piccola azienda e volevo sapere se posso rivolgermi a un investigatore privato per ispezionare il computer aziendale di un mio dipendente.

Anonimo, Monza

Seguendo precisi criteri di proporzionalità, pertinenza e non eccedenza e di rispetto dello Statuto dei Lavoratori si può procedere al controllo del computer aziendale. La posta elettronica aziendale e la connessione internet sono strumenti di lavoro, messi a disposizione dal datore e come tali devono essere utilizzati: evitandone cioè l'uso privato, specie durante l'orario di lavoro. Purtroppo, non sempre è così e spesso i dipendenti ne fanno un uso distorto. Molte aziende però tollerano l'utilizzo della posta elettronica aziendale anche per un ragionevole uso privato. Ciò comporta problemi in quanto sullo stesso account convivono comunicazioni aziendali e personali, creando evidenti difficoltà se si dovesse rendere necessario l'accesso all'intero archivio nell'ambito di una investigazione per verificare l'esistenza di illeciti o inadempimenti commessi dal lavoratore. Altro aspetto che occorre considerare è quello relativo ai principi costituzionali che tutelano la libertà e la segretezza della corrispondenza all'art. 15 e dal codice penale all'art. 616. Da evidenziare è che alcune interpretazioni hanno ritenuto che la posta elettronica non sia da considerare "chiusa", ma "aperta" e pertanto non rientri nella fattispecie disciplinata dall'art. 616 c.p. e, comunque essendo uno strumento aziendale di proprietà del datore di lavoro, protetto da password, il controllo effettuato dal datore di lavoro non costituirebbe un illecito penale. Anche il Garante della Privacy è intervenuto più volte sul tema ed ha stabilito che il datore per poter effettuare controlli debba predisporre una procedura interna con indicate chiaramente le regole per l'utilizzo di internet e della posta elettronica, oltre agli eventuali controlli che si riserva di effettuare nel rispetto dei principi generali di necessità, correttezza, pertinenza e non eccedenza. La procedura, a norma dello Statuto dei Lavoratori, deve essere affissa in luogo accessibile. Il datore ha l'onere di fornire, al momento dell'assunzione dei dipendenti, ogni informazione attinente la raccolta e il trattamento dei dati relativi all'utilizzo di internet e della posta elettronica, nonché al potere di controllo, ordinario e straordinario, e alle relative modalità di esercizio. L'utilizzo inappropriato del computer aziendale da parte del dipendente per fini privati può portare anche alla denuncia penale da parte del datore di lavoro per appropriazione indebita Art. 646 C.P. Esemplare è la condanna in Cassazione di un dipendente di un istituto di credito che durante l'orario di lavoro utilizzando gli strumenti messi a disposizione dall'istituto, svolgeva operazioni finanziarie di investimenti in borsa in proprio per conto di clienti personali.

Mi devo rivolgere a un investigatore per questioni personali. Esiste un tariffario medio per poter valutare meglio le varie opzioni?

Gianni, Brescia

Non esistono delle tariffe imposte. Le tariffe minime furono introdotte nel 1988 per permettere una valutazione di congruità dei prezzi da parte del prefetto. Successivamente le norme europee sulla libera concorrenza dei mercati le ritennero illegittime e furono abolite il 15 novembre 1997 con pubblicazione su G.U. n.289 12-12-1997. Di conseguenza non esistono dei tariffari medi.

*Se avete domande o quesiti per i nostri esperti potete inviarci una e-mail all'indirizzo **mag@federpol.it**. Vi risponderemo privatamente e se di interesse per i lettori pubblicheremo la vostra richiesta su **Federpol Mag**.*

FEDERPOL MAG
N° 6 | 2023

DIRETTORE RESPONSABILE
Laura Elisabetta Reggiani
mag@federpol.it

DIRETTORE EDITORIALE
Luciano Tommaso Ponzi
presidente@federpol.it

IN REDAZIONE
Virna Bottarelli | Cleopatra Gatti
Giorgia Andrei

HANNO COLLABORATO
Alessandro Barca | Jennifer Basso Ricci
Elisabetta Busuito | Antonio De Matteis
Fabio Di Venosa | Fabrizio Farris
Fabrizio Fratoni | Rita Iacono
Laura Giuliani | Calogero Licata
Riccardo Martina | Marco Martorana
Francesco Sardi de Letto | Alfredo Passaro
Vincenzo Ricciuto | Miléne Sicca
Ugo Terracciano

PROGETTO E IMPAGINAZIONE
Giovanni Magistris

IMMAGINI
Adobe Stock

PROPRIETARIO ED EDITORE
FW COMMUNICATION
divisione di Fritz Walter srl

SEDE LEGALE
Borgo Regale, 7 | 43121 Parma
Tel. +39 340 3362710

DIFFUSIONE
abbonamenti@fwcommunication.it

STAMPA
Nuova Effea
Viale Lombardia 51/53
20862 Brugherio (MB)

Registrazione al Tribunale di Parma
n° 3 del 4 aprile 2022

Iscrizione al Registro degli Operatori
di Comunicazione n° 31664
del 15 giugno 2018

FEDERPOL MAG
è Organo Ufficiale di **FEDERPOL**

GLI INSERZIONISTI

L'Ateneo Digitale più scelto in Italia

PEGASO
Università Digitale

Valutato Eccezionale
Con oltre **5.200 recensioni**
Trustpilot

Scopri la nostra
offerta formativa

72
Percorsi di
Laurea

+300
Master I e II livello
Corsi di Alta Formazione e Perfezionamento

Numero Verde
800.185.095

www.unipegaso.it

LAMSERVICE

Informazioni & Servizi per il mondo degli affari

Tutta la documentazione che cerchi è a portata di click

Tutti i Vantaggi di LAM Service in una sola Card!

Servizio Camerale
Info Commerciali
Info Pre-Fido e Post-Fido

WWW.LAMSERVICE.IT

Lam Service Srl
Sede Legale: Via Besana, 10 - 20122 Milano
Centro Operativo: Via Toscana, 12 Int. D1/11 - 20052 Vignate (MI)
Tel. 029587847 - Email: info@lamservice.it - Web: www.lamservice.it