L'IDENTIFICAZIONE DALLE TECNICHE DI VERIFICA DEL DOCUMENTO ALL'APPLICAZIONE DELLE NORME ANTIRICICLAGGIO

PAOLO CARRETTA

SESSIONE

AS4 - POLIZIA GIUDIZIARIA NORME E PRATICA DELL'IDENTIFICAZIONE PERSONALE NEI CONFRONTI DI POLIZIA

09/09/20

L'identificazione

dalle tecniche di verifica del documento all'applicazione delle norme antiriciclaggio

(Paolo Carretta)

Verificare di volta in volta l'attualità della norma, attraverso la consultazione **https://www.normattiva.it/**

Identificare può consistere, secondo tradizione, nel dare un nome ad un volto, di vivente o di cadavere, ma attualmente rileva anche solo per alcuni dati antropometrici (utilizzati per l'apertura cassette di sicurezza, accesso ad un computer) o per il DNA, ovvero, agendo più in profondità, profilare una persona fisica per analizzarne o prevederne, attraverso un trattamento automatizzato dei dati personali: rendimento, situazione economica, salute, preferenze, interessi, affidabilità, comportamento, ubicazione/spostamenti.

01) L'identificazione

L'identificazione può intendersi riferibile all'accertamento dell'identità di una persona, ovvero l'esatta attribuzione alla stessa delle generalità: nome, cognome, luogo e data di nascita, residenza/domicilio/dimora ed eventualmente nazionalità, cittadinanza, professione, stato civile, paternità e maternità, eventualmente codice fiscale (C.F.); alternativamente si configura come una serie di attività, svolte dalla P.G. ma anche da pubblici ufficiali e da medici legali, tese a stabilire l'identità di una persona (vivente) o di una salma. In entrambi i casi *"viene dato un nome ad un volto".* (Paceri R. – *La Polizia Scientifica* – III Edizione Roma 1992). Dato personale deve intendersi lo *strumento tecnico-giuridico* attraverso cui giungere all'identificazione di una persona fisica definita interessato cui si riferiscano i dati personali oggetto di trattamento e di protezione (art. 4, par. 1, p. 1 *General Data Protection Regulation*, Reg. UE 2016/679 – di seguito GDPR).

L'identificazione non è tuttavia necessaria per l'esercizio del diritto di accesso generalizzato (*Freedom of Information Act*, **FOIA** - D.lgs. n. 97/2016 di mod. del D.lgs. n. 33/2013), introdotto per rendere conforme il diritto interno all'art. 10 della *Convenzione europea dei diritti dell'uomo* (art. 5, c. 2, **FOIA**), che spetta a "chiunque", a prescindere dalle sue qualità o condizioni (ad esempio, di cittadino o residente). Poichè l'art. 5, c. 3 stabilisce che tale diritto *"non è sottoposto ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente"* e che la domanda *"non richiede motivazione"* (v. Linee guida A.N.AC e Circ. n. 1/2019 del Ministro per la P.A.), ne deriva che, in linea di principio, l'identificazione del richiedente non sia necessaria ai fini del suo esercizio. Diventa tuttavia indispensabile per la corretta gestione delle domande: per consentire la trasmissione dei dati e documenti richiesti, per la trattazione di quelle seriali o per individuare e qualificare quelle vessatorie. Può quindi essere intesa, ricorrendone i presupposti, come condizione di ricevibilità della

richiesta. In caso di richiesta anonima o da parte di un soggetto la cui identità sia incerta, la PA deve comunicare al richiedente, se possibile, la necessità di identificarsi secondo le modalità previste.
Nei casi di trasmissione per via telematica della domanda – indicata come modalità ordinaria dall'art. 5, c. 3, d.lgs. n. 33/2013 – si applica l'art. 65, c. 1, del d.lgs. n. 82/2005 (Codice dell'amministrazione digitale - CAD). In base a questa disposizione, le domande presentate alle pubbliche amministrazioni per via telematica sono "valide" ed "equivalenti" alle domande sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento, nei seguenti casi:

a) se sono sottoscritte e presentate insieme alla copia del documento d'identità;

b) se sono trasmesse dal richiedente dalla propria casella di posta elettronica certificata;

c) se sono sottoscritte con firma digitale;

d) se il richiedente è identificato con il sistema pubblico di identità digitale (SPID) o la carta di identità elettronica o la carta nazionale dei servizi.

In riferimento alla prima opzione (sub a), è opportuno chiarire che la domanda deve ritenersi validamente presentata in particolare quando siano soddisfatte le seguenti condizioni:

- *che la domanda di accesso sia stata inviata da un indirizzo di posta elettronica certificata o non certificata;*
- *che nel messaggio di posta elettronica sia indicato il nome del richiedente (senza necessità di sottoscrizione autografa);*
- *che sia allegata al messaggio una copia del documento di identità del richiedente.*

02) La procedura identificativa

La procedura identificativa ordinaria si svolge a cura del Pubblico Ufficiale prendendo visione di un documento di riconoscimento e comparandolo con la persona da identificare. Tale identificazione semplificata presuppone che il cittadino ne sia munito, adempimento che, salvo leggi speciali ed eccezioni (soggetti pericolosi o sospetti per l'autorità di P.S.), non è imposto da nessuna norma. L'identificazione di polizia amministrativa è implicitamente prevista (in via generale un potere d'identificazione) dagli artt. 13 e 14 L. n. 689/81. Tale facoltizza gli appartenenti *"agli organi addetti al controllo sull'osservanza delle disposizioni per la cui violazione è prevista la sanzione amministrativa*", nonché *gli ufficiali e gli agenti di polizia giudiziaria*. Pare infatti evidente che, la contestazione e l'accertamento delle violazioni amministrative, passi necessariamente per l'identificazione dei responsabili, persone fisiche e soggetti diversi, oltre che degli eventuali testimoni. La completa identificazione delle persone fisiche implica la conoscenza dei seguenti dati: nome, cognome, luogo e data di nascita, indirizzo della residenza o domicilio, ed estremi documento identificazione (in materia economica o antiriciclaggio anche il C.F.).

La polizia giudiziaria a competenza limitata (o specifica) è quella cui la Legge assegna tali funzioni nei limiti del servizio cui sia destinata e secondo le attribuzioni (specifici reati). Tale funzione viene svolta (art. 57, c.3 cpp) ad es. dagli appartenenti al *Corpo Nazionale dei Vigili del Fuoco,* che hanno specifica competenza, in materia di incendi, ma anche dai verificatori dei pesi e misure, dai funzionari ANAS, dai funzionari IMCTC, dagli ispettori ASL e dagli ispettori doganali. Sono tenuti quindi ad applicare le norme del c.p.p. per tali attività, prescindendo dal fatto che il reato per cui procedono sia specialistico o meno.

L'identificazione ad opera di militari delle FFAA (D.L. 23 mag. 2008, n. 92, conv. in L. 24 lug. 2008, n. 125), viene prevista con riferimento alle sole persone fisiche. Tale può avvenire nel quadro di piani d'impiego per servizi di vigilanza a siti e obiettivi sensibili, oltre che di perlustrazione e pattugliamento in concorso e congiuntamente alle FFPP (art. 7 bis). In tale veste i militari rivestono la qualifica di agente di P.S. e possono procedere, tra l'altro, all'accompagnamento per l'identificazione (art. 15 TULPS).

Nel caso il documento sia scaduto di validità ma venga esibito, un pubblico ufficiale può completare l'identificazione attraverso una dichiarazione a lui resa dal titolare che sottoscriva la fotocopia di tale documento, confermando l'attualità dei dati ivi contenuti (art. 45 DPR n. 445/2000). È comunque, fatta salva per le amministrazioni pubbliche ed i gestori e gli esercenti di pubblici servizi la facoltà di verificare, nel corso

del procedimento, la veridicità e l'autenticità dei dati contenuti nel documento di identità o di riconoscimento[1]. L'assenza della qualifica di P.U. in capo a chi svolge le formalità dell'identificazione e dell'adeguata verifica della clientela, in materia antiriciclaggio (D. Lgs. n 231/2007), rende inapplicabili le ordinarie ipotesi di reato, per il rifiuto di generalità o per chi le fornisce false in tale ambito, facendosi riferimento alla citata legge speciale (art. 55 D.lgs. n. 231/2007). Nei **Contratti pubblici** l'identificazione e le dichiarazioni sostitutive di atto di notorietà da produrre agli uffici della Pubblica Amministrazione o ai gestori o esercenti di pubblici servizi devono essere sottoscritte dall'interessato in presenza del dipendente addetto, ovvero sottoscritte e presentate unitamente a copia fotostatica non autenticata di un documento d'identità del sottoscrittore. Possono essere inviate anche per via telematica nei procedimenti di aggiudicazione di contratti pubblici, nei limiti previsti dal Regolamento (DPR 445/2000). La fotocopia del documento (art. 45 c. 2 DPR n. 445/2000) del dichiarante deve essere considerata elemento costitutivo dell'autocertificazione, costituendone requisito indispensabile e non sanabile (Cons. Stato, Sez. V, 1/ott./2003, n. 5677).

03) Cosa fare

Chiedere, da parte di un pubblico ufficiale nell'esercizio delle sue funzioni (art. 651 cp), alla persona fisica di declinare (cioè riferire verbalmente) le proprie generalità, che consistono nel nome, nel cognome, nella data e nel luogo di nascita, nella residenza, nel proprio status (coniugato/a o celibe/nubile), nella professione e se necessario nella paternità e maternità. Laddove le informazioni vengano richieste ad un soggetto terzo, in occasione di tumulto, pubblico infortunio o pericolo, in flagranza di reato, la legittimazione attiva è del pubblico ufficiale ma anche dell'incaricato di un pubblico servizio (art. 652 cp). L'obbligo può ritenersi assolto anche mostrando un documento di riconoscimento, ma ritirarlo violentemente, prima che il p.u. ne possa esaminarne il contenuto, configura il diniego di fornire indicazioni sulla propria identità per averne impedita alo stesso la lettura.
Rifiutare la consegna del documento di riconoscimento, rectius di identità, agli ufficiali e agenti di Pubblica Sicurezza (che esercitino in concreto e attualmente la funzione) integra la violazione degli artt. 4 T.U.L.P.S. e 294 del Regolamento, ma solo alle persone ritenute pericolose o sospette l'Autorità di P.S. può ordinare di munirsene entro un termine e di esibirla a richiesta, altrimenti procedendosi a fotosegnalazione delle stesse qualora non siano in grado o rifiutino di provare la propria identità. Il rifiuto di esibizione presuppone comunque la disponibilità del documento di riconoscimento, che non è obbligatoria per i comuni cittadini, salvo che non svolgano attività per cui sia contemplato e che richiedano particolari autorizzazioni o abilitazioni, quali la guida di un autoveicolo, la pesca, la caccia etc. In questi casi è generalmente previsto un documento di riconoscimento specifico che attesti un requisito e la sua attualità (es. patente di guida), venendo comminata una sanzione da leggi speciali per chi non lo esibisca o lo esibisca scaduto.

Giurisprudenza

COMPLETEZZA DEI DATI IDENTIFICATIVI - Il rifiuto (di cui all' art. 651 c.p.) va riferito non solo al nome e cognome, ma anche a tutte le altre indicazioni richieste per una completa identificazione (Cass. Pen. 13.5.1948, Cass. Pen. 10.11.1981).
- Non può valere ad escludere la contravvenzione, né la circostanza che il soggetto fornisca una qualche indicazione sulla propria identità personale, senza fornire le complete generalità, né il fatto che la sua identità sia facilmente accertabile (Cass. Pen. 27.2.1998).
- Sussiste la contravvenzione se il rifiuto concerne il luogo di residenza (Cass. Pen. 7.12.1962).
- Sussiste la contravvenzione anche se la persona è conosciuta dal p.u. o possa essere facilmente identificata (Cass. Pen. 30.3.1968, Cass. Pen. 12.2.1970, Cass. Pen. 3.10.1984).
- La contravvenzione sussiste anche quando il p.u. richiedente sia in grado di procurarsi aliunde le notizie sull'identità dell'inquisito (Cass. Pen. 19.4.1974, Cass. Pen. 27.1.1976, Cass. Pen. 18.4.1989). - Le norme relative alla non menzione della paternità e maternità negli atti (art. 2 legge 31 0ttobre 1955, n. 1064), non hanno rilevanza per l'art. 651 c.p. che ha un ambito di applicazione diverso (Cass. Pen. 26.4.1962).
- Il rifiuto di consegnare il documento di riconoscimento (eventualmente posseduto) al pubblico ufficiale (che eserciti in concreto la funzione) non integra il reato di cui art. 651 c.p. che sanziona il rifiuto di fornire indicazioni sulla propria identità, bensì la violazione degli artt. 4 T.U.L.P.S. e 294 reg. (S.C. sez. I Pen. Sent. 22 giugno – 19 settembre 2017, n. 42808).

[1] La carta di identità elettronica e quella cartacea, conformi al D.M. interno 8. nov. 2007 (Regole tecniche della Carta d'identità elettronica), possono essere rinnovate, anche se in corso di validità, entro i 180 gg dalla scadenza.

PRESUPPOSTO DELLA RICHIESTA FORMULATA DAL PU. Il reato non richiede, per essere integrato, nessun presupposto di necessità, ovvero di fondatezza della richiesta (Cass. Pen. 28.4.1955), venendo rimessa al criterio discrezionale del p.u. la facoltà di chiedere a "chiunque", nell'esercizio delle sue funzioni, le generalità e le altre notizie di cui all'art. 651 c.p. (Cass. Pen. 4.2.1952). Ove non fosse chiaro che chi opera sta svolgendo la propria funzione (es. non veste un'uniforme), l'operatore dovrà qualificarsi con chiarezza mostrando la tessera dell'amministrazione di appartenenza e dovrà chiarire bene la denominazione dell'organismo cui appartiene (Carabinieri, Polizia di Stato, Guardia di Finanza, Polizia Locale, guardie venatorie, guardie ecologiche).

DOCUMENTO ESIBITO E REPENTINAMENTE RITIRATO - In tema di rifiuto di indicazioni sulla propria identità personale (art. 651 c.p.), mostrare il documento ritirandolo violentemente, prima che il pubblico ufficiale possa esaminarne il contenuto, configura il reato per aver impedito al pubblico ufficiale di leggerne gli estremi (S.C. Pen. 7.3.1997 - S.C. Pen. 18.6.1997).

MOMENTO IN CUI SI PERFEZIONA IL REATO DI RIFIUTO DI GENERALITA'. Ai fini della consumazione del reato (art. 651 c.p.) è sufficiente il rifiuto di fornire al Pubblico Ufficiale indicazioni circa la propria identità personale, per cui è irrilevante che tali indicazioni vengano successivamente fornite o che l'identità del soggetto sia facilmente accertata per la conoscenza personale da parte del Pubblico Ufficiale o per altra ragione (Trib. Roma, Sez. X, 24.5.2014). - Il reato di rifiuto di generalità, si perfeziona con il semplice diniego di fornire le richieste indicazioni sulla propria identità personale, nulla rilevando, quindi, ai fini della sussistenza dell'illecito, che dette indicazioni vengano fornite in un momento successivo (Cass. Pen., Sez. VI, 6.11.2006, n. 41716). - Il reato di rifiuto di generalità si perfeziona con il semplice diniego di fornire le richieste indicazioni sulla propria identità personale, non rilevando, ai fini della sussistenza dell'illecito, che dette indicazioni vengano fornite in un momento successivo (Cass. Pen. 18.6.1997, Cass. Pen. 9.1.1985). Il reato previsto dall'art. 651 c.p. - rifiuto di indicazioni sulla propria identità personale - è istantaneo, in quanto si consuma nel momento stesso in cui il soggetto attivo, che ne sia stato legittimamente richiesto, rifiuti di dichiarare la propria identità, giacché tale condotta produce di per sé la lesione del bene tutelato dalla norma incriminatrice, vale a dire l'ordine pubblico inteso come interesse generale a evitare ogni intralcio all'attività dei pubblici ufficiali preposti istituzionalmente all'assolvimento di compiti di prevenzione, accertamento o repressione dei reati o di garanzia della pace e della tranquillità pubblica. È del tutto irrilevante, perciò, che il pubblico ufficiale possa accertare in altro modo l'identità del destinatario del suo ordine, così come è irrilevante l'eventuale ripensamento della persona interpellata, che dopo un iniziale rifiuto, si risolva, finalmente, a indicare le proprie generalità (Cass. Pen., 25.5.1995, n. 6052). - I conducenti di veicoli sono tenuti a dare le generalità al pubblico ufficiale che le abbia richieste e l'erronea persuasione che le indicazioni siano contenute nel libretto, già in possesso dell'agente, non esclude né la sussistenza né la punibilità del reato (Cass. Pen. 24.2.1961). - Quanto all'elemento soggettivo del reato, trattandosi di contravvenzione è sufficiente la colpa non occorrendo la conoscenza, ma bastando la semplice rappresentabilità della qualità di pubblico ufficiale nel richiedente. Ad escludere il reato, poi, non è necessario che la richiesta integri un atto arbitrario del pubblico ufficiale, essendo sufficiente la mera illegittimità (Cass. Pen. 23.2.1977). – Il reato di rifiuto di generalità si perfeziona con il semplice diniego di fornire le richieste indicazioni sulla propria identità personale, nulla rilevando, quindi, ai fini della sussistenza dell'illecito, che dette indicazioni vengano fornite in un momento successivo (Cass. Pen., Sez. I, 26.9.1997, n. 8624).

LA CANCELLAZIONE DELLE SOCIETA' DI CAPITALI E DI PERSONE dal Registro delle Imprese ha effetto estintivo immediato. Gli atti successivi a tale evento non possono essere collettivamente notificati ad amministratori e soci e/o al liquidatore. In tale ipotesi saranno anche tali soggetti persone fisiche a dover essere identificati (Cass. S.U. n. 4062/2010) riconducendo tali dati alla società.

UFFICIALE/AGENTE DI PG PARTE IN CAUSA O FUORI SERVIZIO. L'appartenente alla Polizia che, alla guida della propria autovettura, sia coinvolto in fatti di circolazione stradale, può nella veste di ufficiale di polizia giudiziaria, ove rilevi la ricorrenza degli estremi di un reato, procedere all'identificazione della persona, autrice di esso, richiedendo alla stessa indicazioni sulla sua identità personale. Qualora il soggetto richiesto rifiuti di fornire le generalità, risulta integrato il reato di cui all'art. 651 c.p. (Cass. Pen. 29.3.1971).

ESSERE PERMANENTEMENTE IN SERVIZIO da parte di un appartenente alle FFPP implica una situazione di fatto diversa da un esercizio (attuale) delle funzioni del proprio ufficio, prevedendosi che il pubblico ufficiale possa in ogni momento intervenire per esercitarle, pur non trovandosi concretamente ad essere comandato in servizio. Gli appartenenti alla (ora) Polizia di Stato "in servizio permanente" sono sempre tenuti, come appartenenti alla Polizia giudiziaria, anche se liberi dal servizio, ad accertare i reati e le infrazioni amministrative. Ne consegue che il rifiuto opposto alla richiesta di un assistente di Polizia di fornire le generalità integra il reato previsto dall'art. 651 c.p. (Cass. Pen., 24.3.2003, n. 11709). In applicazione di tale quadro normativo, la S.C. ha tuttavia coerentemente confermato l'esclusione della configurabilità del reato di cui all'art. 651 c.p. in un caso in cui un ufficiale della polizia stradale, senza contestare alcuna specifica infrazione, aveva chiesto, senza ottenerle, le generalità al conducente di una macchina operatrice, dopo che questi aveva effettuato una manovra che aveva intralciato la marcia del veicolo privato sul quale il detto ufficiale in quel momento si trovava, quale passeggero (Cass. Pen. 8.10.1993 e 17.4.2001). Il reato di cui all'art. 651 c.p., sussiste tuttavia nell'ipotesi di rifiuto di indicazioni sull'identità personale, richieste da un maresciallo dei CC, anche se il sottufficiale sia in licenza, in località diversa da quella di servizio e sia inopportunamente intervenuto direttamente su richiesta di un congiunto, per un reato perseguibile a querela, prima che questa sia stata presentata (S.C. Pen. 13.10.1977).

GUARDIE VENATORIE, GUARDIE ZOOFILE; CONTROLLORI DEL TRASPORTO PUBBLICO. Le guardie venatorie, nell'esercizio delle loro funzioni non sono agenti di pg ma pubblici ufficiali, esercitando poteri autoritativi e certificativi per lai protezione della fauna selvatica, patrimonio indisponibile dello Stato. Integra il reato ex art. 651 c.p. il rifiuto a tali soggetti delle proprie generalità (Cass. Pen. Sez. V, 23.5.1997, n. 4898). Le guardie zoofile (che non rivestono più la qualifica di agenti di PS ex art. 5 del DM 31 marzo 1979), hanno attualmente la qualifica di guardie giurate, quindi PU ai sensi dell'art. 57 cpp., artt. 133 e 134 del RD 18 giugno 1931, n. 773 (S.C. Sez. I, 30.11.1996, n. 10282). La legge 11 febbraio 1992 n. 157, art 27 c.1, ha affidato la vigilanza venatoria: a) agli agenti dipendenti degli enti locali delegati dalle regioni. b) alle guardie volontarie delle associazioni venatorie, agricole e di protezione ambientale nazionali

presenti nel Comitato tecnico faunistico-venatorio nazionale e a quelle delle associazioni di protezione ambientale riconosciute dal Ministero dell'ambiente, alle quali sia riconosciuta la qualifica di guardia giurata. Ai soli agenti dipendenti degli enti locali delegati dalle regioni, di cui alla lett. a) è stata però riconosciuta la qualifica di agenti di polizia giudiziaria e di pubblica sicurezza (Consiglio di Stato Sez. VI sent. 298 del 26 gennaio 2007). Il controllore dei pubblici servizi di trasporto, nell'atto di richiedere il titolo di viaggio ai passeggeri o di verificarne la validità, riveste la qualità di pubblico ufficiale (S.C. Pen. 24.1.1975).

04) Esaminare un documento di riconoscimento

Esaminare il documento di riconoscimento (di cui *quello d'identità costituisce specie* ex D.P.R. 445/2000) ove la persona, dopo la richiesta, opti per la sua esibizione, impone anzitutto una verifica della sua genuinità, vale a dire che non abbia subìto alterazioni (modifica di un documento regolare) o contraffazioni (documento falso *ab initio*) che ne determinerebbero la falsità materiale; esempio tipico è la sostituzione della fotografia, che suggerisce un'errata associazione tra tratti somatici raffigurati e generalità riportate.

Furto di identità viene intesa: *l'impersonificazione totale* attraverso occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'*identità e al reddito* di altra persona, vivente o deceduta; *l'impersonificazione parziale* attraverso un occultamento che combini dati personali propri con l'utilizzo indebito di quelli altrui, nelle stesse ipotesi. Il MEF gestisce il *sistema pubblico per la prevenzione del furto di identità* (D.lgs.11 aprile 2011, n. 64), il cui *archivio centrale informatizzato* consente a banche, finanziarie, fornitori di servizi di comunicazione elettronica e interattivi, imprese di assicurazione, fornitori di energia e gas, di verificare l'autenticità dei dati contenuti nei documenti di identità e di reddito delle persone fisiche che richiedano prestazioni nell'ambito dei servizi che offrono. La verifica avviene attraverso il riscontro coi *data base* di amministrazioni ed enti pubblici: Agenzia delle Entrate, INAIL, INPS, Ministero dei trasporti e delle Infrastrutture, Ministero dell'interno, Ragioneria Generale dello Stato. L'archivio centrale può essere consultato dalle FFPP per analizzare fenomeni criminali e prevenire reati finanziari. Al sistema partecipano i soggetti destinatari degli obblighi antiriciclaggio di *adeguata verifica della clientela*.

Gli addetti ai servizi d'informazione per la sicurezza (AISE, AISI) potrebbero esibire ad un controllo documenti di identificazione o di riconoscimento che, pur essendo ideologicamente falsi, ovvero contenenti indicazioni di qualità personali diverse da quelle reali, possono essere utilizzati purchè non attestanti le qualità di ufficiale o agente di polizia giudiziaria, tributaria o di pubblica sicurezza. Escludendo l'ipotesi di cui sopra, perché tale uso risulti lecito, come pure l'utilizzazione di documenti e certificati di copertura, deve essere sempre rispettata la particolare procedura di cui all'art. 24 della l. 3/8/2007, n. 124 che reca la nuova disciplina del segreto e la riforma dei servizi d'informazione per la sicurezza. Presso il DIS è tenuto un registro riservato e, al termine dell'operazione, il documento o il certificato è conservato in apposito archivio (art. 4). La stessa legge prevede (art. 25) l'esercizio di attività economiche simulate. L'esercizio può avvenire sia nella forma di imprese individuali sia nella forma di società di qualunque natura. Il regolamento stabilisce le modalità di svolgimento di tali attività.

Le operazioni sotto copertura, limitate alle tre maggiori FFPP, sono previste per contrastare: riciclaggio, reimpiego, delitti contro la libertà personale, delitti concernenti *armi*, *munizioni e esplosivi*, *immigrazione clandestina*, *sfruttamento e induzione alla prostituzione*, *delitti commessi con finalità di terrorismo*, *estorsione*, *usura*, *contraffazione* (art. 9, L. n. 146/2006) e taluni reati contro la P.A. La c. d. spazzacorrotti (art. unico, c. 8, L. n. 3/2019) ha previsto tale ultima possibilità, modificando i reati presupposto e le condotte scriminate (art. 9 L. 146/2006). Per l'esecuzione di tali operazioni (art. 9, c. 1 e 2), gli UPG possono avvalersi di agenti di PG, di ausiliari e di interposte persone, ai viene estesa la causa di non punibilità. Per l'esecuzione delle operazioni è possibile l'utilizzazione temporanea di documenti di copertura (falsi), l'attivazione di siti nelle reti, la realizzazione e la gestione di aree di comunicazione o scambio su reti o sistemi informatici. In tale ambito *le identità di copertura* possono essere utilizzate per entrare in contatto con soggetti e siti nelle reti di comunicazione, informandone, comunque entro le 48 ore dall'inizio dell'attività, il P.M. L'identità degli agenti *undercovered* (art. 9 L. cit).) è oggetto di particolare attenzione, prevedendosi per la sua rivelazione una pena severa.

Collaboratori di giustizia e testimoni di cui al programma speciale di protezione (D.M. n. 161 del 23 apr. 2004, art. 8 n. 4) utilizzano documenti di copertura, perché siano assicurati la loro sicurezza, la riservatezza e il reinserimento sociale. Questo implica la possibilità che per l'identificazione operata dalle FF.PP. vengano esibiti dagli interessati documenti ideologicamente falsi, o riferibili al loro cambiamento di generalità (D.lgs. 29/mar. /1993 n. 119). Il controllo per l'utilizzo di tali documenti di riconoscimento compete al Servizio centrale di protezione, salvaguardando la riservatezza delle informazioni.

05)Strumenti e tecniche

L'autenticazione informatica è possibile attraverso componenti hardware e programmi informatici, che prevedono l'utilizzo da parte dell'utente di credenziali di autenticazione consistenti in dati e dispositivi, in suo possesso, noti o allo stesso univocamente correlati, utilizzabili per farsi riconoscere. Tali credenziali sono quindi costituite da qualcosa che **conosce** (una password: stringa di caratteri alfanumerici liberamente scelta e all'utente associata), **possiede** (un *PIN*, una *smart card*, un *token* dal quale ottenere una password dinamica), **è** (credenziale biometrica correlata alla persona).
I dati biometrici non rappresentano una garanzia assoluta in quanto una stampante 3D, il trucco cosmetico o una foto possono ingannare i sistemi che utilizzano per l'autenticazione le impronte digitali o il riconoscimento facciale, realizzando fenomeni di *spoofing* (falsificazione dei dati biometrici). In ogni caso sono dati personali esistenti che vengono correlati ad un soggetto, all'interno di una banca dati o attraverso un documento e devono essere presi in considerazione per l'identificazione con la dovuta cautela. Le principali credenziali biometriche utilizzate sono: **impronta digitale** per cui esiste un discreto rischio di frode e qualche esperto riesce ad ingannare i sistemi di rilevamento attraverso impronte a base di gelatina per l'80% dei casi, ad es. sistema *Fido* (Fast Identity Online Alliance) che opera su PayPal attraverso tablet o smart phone; **l'iride** che è la zona colorata dell'occhio, composta da oltre 260 punti caratteristici, e presenta un rischio di frode basso; **geometria del palmo della mano** che prevede il rilevamento di oltre 90 misure che vengono digitalizzate e comparate, presenta un basso rischio di frode; **il riconoscimento facciale in 3D e iride** a distanza che è utilizzato da *Morpho* un tablet multi biometrico consente una verifica incrociata che rafforza il sistema**; verifiche biometriche incrociate di voce e volto** connotano certi videofonini; **segnali cardiaci e cerebrali** caratterizzano il sistema *Starlab*; **un sistema integrato di riconoscimento di volto, voce, documento d'identità e carta di credito** viene utilizzato da *Facebanx*; **il battito cardiaco** che consente una protezione efficace, si configura come una credenziale biometrica correlata in una banca dati, divenendo riconoscibile e confrontabile, leggibile attraverso un elettrocardiografo. La tendenza è quella di integrare qualsiasi sistema di riconoscimento biometrico con i prodotti tecnologici di uso comune, in modo che l'utente abilitato possa identificarsi nel modo più semplice. Un braccialetto biometrico (già disponibile) comunica i dati attraverso *bluetoot* all'apparato cui si vuole accedere. Le **password** diventano credenziali di riserva, da utilizzare in caso di malfunzionamento dei sistemi.
Il LOG (ing. diario di bordo) registra, nel computer (log-file o file-log) e nei server, i principali accadimenti della navigazione nel WEB. L'operazione di registrazione (LOG) dell'internauta, previa autenticazione, viene effettuata automaticamente e prevede una verifica secondo impostazioni predisposte dall'amministratore di rete. Vale per l'accesso ad un qualsiasi sistema informatico, salvo accorgimenti più o meno leciti che possono rendere difficoltosa o addirittura inibire tale identificazione.

06)Documenti- nota esplicativa

L'identificazione può avere finalità di prevenzione, **ma anche repressive**, in materia amministrativa o penale, prevedendosi a tal fine l'utilizzo strumentale di un documento di identità (la carta di identità di seguito C.I.) o di riconoscimento che, qualora ne contenga i dati, viene detto equipollente (alla C.I.) ex D.P.R. 28.12.2000, n. 445 - Art. 35. Tale non può essere considerata ad es. la tessera d'appartenenza alle FFPP per

risultare mancante la residenza. In tutti i casi in cui nel T.U. viene richiesto un documento di identità, esso può sempre essere sostituito dal documento di riconoscimento equipollente (c. 2). Tali sono considerati il passaporto, la patente di guida, la patente nautica, il libretto di pensione, il patentino di abilitazione alla conduzione di impianti termici, il porto d'armi, le tessere di riconoscimento, purché munite di fotografia e di timbro o di altra segnatura equivalente, rilasciate da un'amministrazione dello Stato. Nei documenti d'identità e di riconoscimento non è necessaria l'indicazione o l'attestazione dello stato civile, salvo specifica istanza del richiedente.

La carta d'Identità è il tipico documento di identificazione, previsto dall'art. 3 del TULPS, R.D. 773/1931 e art. 288 del Regolamento - TULPS oltre che dall'art. 35 del DPR 445/00. L'articolo 10 del decreto-legge 13 maggio 2011 n. 70, recante "*Prime disposizioni urgenti per l'economia*", ha innovato le disposizioni in materia di rilascio di C.I., modificando l'articolo 3 del TULPS, R.D. 773/1931. Viene soppresso il limite di età minimo per il rilascio della C.I., precedentemente fissato in quindici anni, ed è stabilita una validità temporale diversa di tale documento, a seconda dell'età. La C.I. è rilasciata ai cittadini fin dalla nascita. Ha validità di: tre anni per i minori di anni 3; cinque anni per coloro che hanno una età compresa tra i 3 anni (compiuti) e i 18 anni (non ancora compiuti); dieci anni per i maggiori di anni 18 e scade nel giorno del proprio compleanno. La carta d'identità dovrà riportare la firma del titolare che abbia compiuto dodici anni, salvo i casi di impossibilità a sottoscrivere. Per i cittadini italiani equivale al passaporto ai fini dell'espatrio nell'UE e in quelli con cui vigono particolare accordi internazionali. Per chi sia residente in altro comune ma abbia il domicilio in quello in cui presenta la richiesta, il rilascio o il rinnovo della carta d'identità può avvenire con documento precedente già scaduto, smarrito o rubato, e per gravi e comprovati motivi che gli impediscano di recarsi presso il proprio comune di residenza, allegando la relativa documentazione. La richiesta di rilascio della C.I. come cittadino residente in altro comune, comporta l'iscrizione nell'Anagrafe dei "temporaneamente residenti" di quello di rilascio, e può dare luogo a successivi controlli sulla abitualità della dimora e all'eventuale iscrizione d'ufficio nell'Anagrafe della Popolazione Residente. Il servizio viene erogato previa autorizzazione del comune di residenza. In caso di smarrimento o furto della carta di identità precedente, al momento della richiesta occorre presentare la denuncia e, nel caso non si fosse in possesso di altro documento d'identità in corso di validità, al momento del rilascio della nuova C.I., occorre presentarsi con due testimoni maggiorenni muniti di documento di identità valido.

La Carta di Identità Elettronica (CIE) consente un innovativo rapporto con la P.A. qualora utilizzata quale strumento di autorizzazione all'accesso informatico, ma è anche un affidabile strumento di identificazione, contenendo i dati personali necessari e il codice fiscale (C.F.) dei cittadini. Con tale documento polivalente si viene abilitati ad accedere ai servizi online locali e nazionali attraverso un'autenticazione elettronica: firma digitale, servizi sanitari, prenotazioni, pagamenti. Nella banda ottica contiene l'immagine dell'impronta del dito indice della persona, come previsto dal TULPS. Per garantire la riservatezza e la sicurezza dei dati, oltre che per ridurre il rischio di falsità materiale, vengono utilizzati sistemi definiti di *strong authentication* e *template* (modello predefinito) criptati dell'immagine dell'impronta digitale. Si avvale di una procedura messa punto dall'Eba (*European Banking Authority*) che utilizza un doppio fattore di autenticazione attraverso differenti elementi di categorizzazione dei codici riservati, che solo il soggetto conosce. Un set di codici attiene alla conoscenza personale: un *knowledge code*. Il secondo comprende un elemento di possesso: il *possession code*. Un ulteriore set di codici comprende ciò che la persona è: *inherence* (dati correlati). Questi tre set sono interdipendenti; anche se uno dovesse essere scoperto da un soggetto terzo, gli altri rimangono scorrelati e non sono deducibili. l'impronta biometrica di riferimento viene correlata attraverso la *registrazione dell'utente*, conosciuta anche come fase di *enrollment*. Viene così creato un *template* con l'acquisizione dell'immagine relativa all'individuo, elaborata con un algoritmo, memorizzato nel sistema e reso confrontabile nella *fase di autenticazione*. La ***CIE*** potrà essere richiesta solo dai cittadini italiani o stranieri residenti nel Comune ove si chiede il rilascio e del codice fiscale, che non siano in possesso di carta di identità anche cartacea (anche rilasciata da altro Comune) con un residuo di validità superiore a sei mesi, con l'unica eccezione delle C.I. valide per l'espatrio prorogate in caso l'interessato debba recarsi all'estero.

La Carta d'identità di modello europeo, di prossima adozione (2 anni), introduce requisiti minimi comuni, uniformando quantità e tipologia di informazioni contenute, prevedendosi: validità minima anni 5 e massima 10, maggiore di 10 anni per gli ultrasettantenni e minore di 5 ai minori. Il modello (ID-1) avrà il formato delle carte di credito, con una zona funzionale a lettura ottica (conformità alle norme minime di sicurezza - Organizzazione per l'aviazione civile internazionale), bandiera UE e codice dello stato emittente. Conterrà inoltre una foto e due impronte del titolare, conservate in formato digitale «su un microchip senza contatto».
Il passaporto ordinario è valido per tutti i Paesi i cui Governi siano riconosciuti da quello Italiano. È rilasciato ai cittadini italiani e ha durata decennale. Dal 26 ottobre 2006 viene rilasciato il passaporto elettronico. Ai sensi dell'art. 1 della L. 21 novembre 1967, n. 1185, ogni cittadino è libero, salvi gli obblighi di legge, di uscire dal territorio dello Stato, valendosi del passaporto o documento equipollente (quando consentito). In aderenza alla vigente normativa UE, dal 20 maggio 2010 viene rilasciato ai cittadini, da tutte le Questure in Italia ed all'estero dalle rappresentanze diplomatiche e consolari, un passaporto elettronico costituito da un libretto di 48 pagine a modello unificato, dotato di un microchip in copertina, contenente i dati anagrafici, la foto e le impronte digitali del titolare. Alla pagina 2 si trova la firma digitalizzata, fatta eccezione per i minori di anni 12, gli analfabeti e coloro che presentino una impossibilità fisica accertata e documentata che ne impedisca l'apposizione. In questi casi al posto della firma compare la dicitura "esente" anche in lingua inglese e francese. Per i minori oltre ai cambiamenti già intervenuti, è ora previsto che siano tutti dotati di un passaporto individuale, pertanto non ricorre più l'iscrizione del figlio minore sul passaporto del genitore. I dati biometrici raccolti (immagine del volto e impronte degli indici delle due mani) vengono inseriti nel chip per la verifica dell´autenticità del documento e dell´identità del titolare; l´utilizzo di tali dati biometrici avviene "*attraverso elementi comparativi direttamente disponibili*" (in pratica confrontandoli con la persona ma non vengono raccolti, correlati e conservati in una banca dati centralizzata e questo rappresenta un grosso limite sotto il profilo di polizia. La Banca Dati passaporti (D.M. 31 marzo 2006) consente solo la verifica dell'esistenza di precedenti passaporti rilasciati alla medesima persona, ovvero dei dati del passaporto oggetto di furto o smarrimento nonché le verifiche in caso di malfunzionamento del chip. Il *chip* comunica con tecnologia RFID (*Radio Frequency Identification*), in modalità wireless i dati del microchip (*trasponder*) al ricevitore sino a circa 10 cm di distanza. Apposite custodie possono evitare la clonazione inibendo la RFID.
I passaporti speciali, diplomatici e di servizio, di cui al decreto del Ministero degli affari esteri del 5 aprile 2005, che integra il decreto 23 dicembre 2004, n. 1679-bis, rispettano analoghe prescrizioni tecniche.
La patente di guida è un'autorizzazione amministrativa necessaria per la conduzione su strade pubbliche di veicoli a motore, che viene rilasciata dopo che siano stati accertati i requisiti psicofisici, morali e attitudinali della persona. Per poter guidare in paesi stranieri, a volte viene richiesta l'esibizione della patente di guida "nazionale" (rilasciata cioè dal paese di residenza) congiuntamente ad una traduzione ufficiale denominata *permesso internazionale di guida*. La patente di guida tipo card è idonea all'identificazione in quanto l'identità personale può essere dimostrata con ogni documento munito di fotografia rilasciato da un'Amministrazione dello Stato con le caratteristiche di cui al DPR 445/2000, ma non è equipollente.
L'Identità digitale o SPID (D.P.C.M. 24 ottobre 2014) attraverso il Sistema Pubblico di Identità Digitale permette l'accesso ai servizi online della Pubblica Amministrazione con un'unica coppia: *utente – password*. Deve essere intesa quale rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al citato D.P.C.M. e dei regolamenti attuativi, corrispondenti a quelli previsti dalla normativa antiriciclaggio ad opera di una banca, di Poste Italiane o ente equivalente. Può consentire un'identificazione indiretta del soggetto attraverso smartphone, ma non ha le caratteristiche del documento di riconoscimento.
Si verifica interrogando le banche dati (quando possibile) la corrispondenza dei dati personali, ma anche l'esistenza di provvedimenti pendenti, principalmente lo SDI (se procede la G.d.F. anche A.T.). L'accesso ai dati ed informazioni dello SDI e il loro uso (art. 9 legge 121/1981) sono consentiti agli ufficiali di polizia giudiziaria appartenenti alle forze di polizia, agli ufficiali di pubblica sicurezza e ai funzionari dei servizi di sicurezza, nonché agli agenti di polizia giudiziaria delle forze di polizia debitamente autorizzati (art.11). L'accesso ai dati e alle informazioni è consentito all'A.G. ai fini degli accertamenti necessari per i procedimenti

in corso e nei limiti stabiliti dal c.p.p. Risulta vietata ogni utilizzazione delle informazioni e dei dati per finalità diverse da quelle previste (dall'art. 6 lett. a). Resta vietata la circolazione delle informazioni all'interno della P.A. fuori dei casi previsti. Gli accessi abusivi, pur da parte di operatori (soggettivamente) abilitati, sono sanzionati ex art. 615-*ter* c.p. (*accesso abusivo ad un sistema telematico od informatico*).

07)Interpol - le notizie a stampa nell'identificazione di persone

Interpol implementa il sistema delle notizie a stampa o Interpol notice, che vengono pubblicate e diffuse in tutti i Paesi membri, a richiesta, dopo il loro controllo contenutistico e formale, nonché l'implementazione della banca dati nazionale. Sono accessibili on-line da parte degli operatori di polizia e risultano suddivise in due macro-categorie:

- **colour-coded notice**, ovvero alert inseriti nel canale Interpol, il cui contenuto informativo è associato ad un colore identificativo, per l'immediata classificazione operativa del dato;
- **special notice**, non catalogabili tra le coluor-coded, ma emesse nell'ambito di specifici strumenti di cooperazione approvati dall'ONU.

La relativa base giuridica è nello statuto O.I.P.C.-Interpol, e nel relativo Regolamento sul trattamento dei dati.
Una notizia a stampa contiene: elementi identificativi del segnalato (i.e. foto, impronte digitali, stato civile, doc. identità, segni particolari, lingua, stati frequentati), elementi giuridici della fattispecie (qualificazione del reato, pena inflitta o cornice edittale del reato, a seconda della legislazione del Paese inseritore).
Vengono pubblicate su richiesta degli Uffici Centrali Nazionali e rese disponibili con la pubblicazione sul sito internet dell'Interpol. Non possono perseguire finalità di natura politica, militare, religiosa o razziale (art. 3 della Costituzione dell'O.I.C.P.
Le notice vengono utilizzate dall'ONU, da Tribunali Penali Internazionali e dalla Corte Penale Internazionale, al fine di ricercare soggetti indagati per la commissione di crimini commessi nelle rispettive giurisdizioni: genocidio, crimini di guerra o crimini contro l'umanità. Vengono classificate in base al colore (**colour-coded**):

- **rosso** quelle finalizzate a richiedere la localizzazione e l'arresto di una persona ricercata da un'AG o da un tribunale per fini estradizionali; come specificato dall'art. 83 del Reg., possono essere pubblicate solo qualora riguardino un reato grave o comune, essendo esclusi fatti inerenti violazioni civili e/o amministrative, salvo che queste ultime siano finalizzate a favorire la commissione di un illecito penale o siano connesse a fatti di criminalità organizzata; contengono gli estremi del provvedimento restrittivo e dell'A.G. emittente.
- **giallo** quelle finalizzate ad individuare una persona scomparsa o ad indentificare un individuo incapace di identificare sé stesso; possono confluire nel canale Interpol solo previa denuncia alla competente autorità di polizia nazionale, non devono essere ostacolate dalla legge nazionale sulla privacy qualora riguardino una persona adulta;
- **blu** quelle volte a localizzare, identificare o ottenere informazioni su una persona ritenuta d'interesse nell'ambito di un procedimento penale qualora risulti indagata, imputata, testimone o vittima;
- **nero** quelle preposte ad ottenere informazioni su cadaveri non identificati;
- **verde** quelle volte a mettere in guardia in merito ad attività criminali di una persona nel caso questa sia considerata un possibile pericolo per la sicurezza pubblica; quando gli uffici nazionali (U.C.N.) ricevono green notice, le competenti Autorità di polizia nazionali devono attivarsi, in conformità al diritto interno, per intraprendere adeguate contromisure (art. 89 Reg.);
- **arancione** quelle finalizzate ad informare in merito ad una persona, un evento, un oggetto o un procedimento che rappresenti una minaccia o un pericolo imminente per l'incolumità fisica e/o giuridica di persone o cose
- **viola** quelle inserite per fornire informazioni su modus operandi, procedure, oggetti, congegni o nascondigli utilizzati da malviventi, risultando divulgabili solo qualora la pertinente indagine sia conclusa, salvo si tratti di investigazioni afferenti reati gravi o sia di particolare interesse investigativo per le forze di polizia di altri Paesi;
- **le notizie speciali** Interpol-Consiglio di Sicurezza UN hanno lo scopo di informare gli operatori che su una persona fisica o giuridica gravano sanzioni delle Nazioni Unite (UN).

08)Pratiche per l'identificazione di persona fisica

Il fotosegnalamento viene effettuato presso l'autorità di P.S., che ha facoltà di ordinare che le persone pericolose o sospette e coloro che non sono in grado o si rifiutano di provare la loro identità siano sottoposti a rilievi segnaletici (art. 4 R.D. 18 giu. 1931, n. 773, TULPS). Tali rilievi per le persone pericolose o sospette e per coloro che non siano in grado o si rifiutino di provare la propria identità, giusta l'art. 4 del TULPS, sono descrittivi, fotografici, dattiloscopici e antropometrici (art. 7 R.D. 6 mag. 1940, n. 635).

Alimenta il sistema AFIS (*Automatic Fingerprint Identification System*) per il Casellario Centrale della Polizia Scientifica del Ministero dell'Interno, settore sistemi biometrici dattiloscopici. Vengono acquisiti e registrati nel *data base* i cartellini fotosegnaletici e le impronte digitali di tutti i fotosegnalati, inclusi i detenuti, ed è esteso ai dati dei richiedenti di permesso di soggiorno, risultando integrato col sistema europeo *Eurodac* che gestisce le richieste di asilo politico agevolando la cooperazione internazionale di polizia (vds oltre).

Un sistema per il riconoscimento vittime (ADVIS) per la polizia scientifica, raccoglie i dati delle persone scomparse, per finalità di ricerca ma anche di identificazione cadaverica in caso di incidenti/rinvenimenti che vedano coinvolte persone non note. I relativi parametri sono condivisi dalle polizie europee, consentendo ai medici legali la verifica d'identità con la comparazione dei dati mediante un motore di ricerca.

La Banca dati nazionale del DNA, (c/o *il Ministero dell'interno – Dipartimento della pubblica sicurezza*) istituita con L. n. 85/2009 (di adesione trattato di Prüm, in ossequio alle *Decisioni quadro del Consiglio dell'Unione europea* 2008/615/GAI e 2008/616/GAI, per il contrasto del terrorismo e della criminalità transfrontaliera) raccoglie e conserva (per 20 anni, ma i profili acquisiti a seguito di assoluzione con formula piena vengono cancellati al verificarsi del fatto) i dati forniti dal **Laboratorio centrale** (c/o *il Ministero della giustizia - Dipartimento dell'amministrazione penitenziaria*), agevolando l'identificazione delle persone indagate in ambito criminale (art. 5), oltre che dei cadaveri. Il Codice Univoco Identificativo (**CUI**) è alfanumerico, generato in automatico dal **sistema AFIS** (di cui oltre) e legato univocamente alla persona (art. 9 L. cit) o al consanguineo sottoposti a prelievo di un campione biologico (Regolamento: DPR n. 87/2016). Attraverso tale sistema viene resa possibile la comparazione dei profili del DNA di indagati, già implicati in procedimenti penali, con i profili rinvenuti/ottenuti dalle tracce biologiche presenti sulla scena di un crimine. Le FFPP custodiscono, per la consultazione e i raffronti, i dati relativi ai profili, mentre compete alla citata articolazione del Ministero della Giustizia (**Dap**) l'estrazione del profilo del DNA, oltre all'implementazione telematica della banca dati nazionale o **BDN - DNA**. Il Comitato nazionale per la biosicurezza, le biotecnologie e le scienze della vita (**CNBBSV**) garantisce l'osservanza dei criteri e delle norme tecniche per il funzionamento del laboratorio centrale e vi esegue, sentito il Garante per la protezione dei dati personali, le necessarie verifiche oltre che presso i laboratori che lo alimentano. La legge (art. 14) punisce con la reclusione da uno a tre anni le violazioni dolose concernenti l'utilizzo improprio di tali dati, fino a sei mesi quelle colpose, affidando al *Garante per la protezione dei dati personali* il controllo sulla **BDN - DNA** (art. 15) cui compete (art. 7) il raffronto del DNA a fini identificativi. La raccolta dei profili del DNA riguarda quindi:

- le persone sottoposte a misure restrittive della libertà personale (art. 9, c. 1), con la precisazione che, in caso di arresto in flagranza di reato o di fermo di indiziato di delitto, il prelievo può essere effettuato solo dopo la convalida da parte del giudice; i soggetti detenuti o internati a seguito di sentenza irrevocabile, per un delitto non colposo; i soggetti nei confronti dei quali sia applicata una misura alternativa alla detenzione a seguito di sentenza irrevocabile, per un delitto non colposo; i soggetti ai quali sia applicata, in via provvisoria o definitiva, una misura di sicurezza detentiva;
- la raccolta dei dati relativi ai reperti biologici acquisiti nel corso di procedimenti penali (art. 10), ma è escluso ove si proceda nei seguenti casi (art. 9, c. 2): … *a) reati di cui al libro II, titolo III, capo I, tranne quelli di cui agli articoli 368, 371-bis, 371-ter, 372, 374 aggravato ai sensi dell'articolo 375, 378 e 379, e capo II, tranne quello di cui all'articolo 390, del cp; b) reati di cui al libro II, titolo VII, capo I, tranne quelli di cui all'articolo 453, e capo II, del cp; c) reati di cui al libro II, titolo VIII, capo I, tranne quelli di cui all'art. 499, e capo II, tranne quello di cui all'art. 513-bis cp; d) reati di cui al libro II, titolo XI, capo I, del cp; e)* ***reati fallimentari*** *di cui al r.d. 16*

marzo 1942, n. 267; f) reati previsti dal codice civile; g) ***reati in materia tributaria****; h) reati previsti dal testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al d.lgs. 24 febbraio 1998, n. 58;*
- la raccolta dei dati dei profili di persone scomparse, di loro consanguinei e di cadaveri/resti non identificati.
Il laboratorio centrale per la banca dati nazionale del DNA ha invece il compito (art. 8):
- la tipizzazione del profilo del DNA dei soggetti indicati dalla legge;
- la conservazione dei relativi campioni biologici da usare per tipizzare i profili di DNA.
L'art. 224 bis cpp prevede i casi e i modi del prelievo, nell'ambito della perizia. Considerando che tale attività implica il compimento di atti idonei ad incidere sulla libertà personale, risulta utile considerare la possibilità di procedere a prelievi coattivi su persone diverse dall'indagato, disponendo la norma (art. 224-bis, c. 3 cpp) sia per *l'imputato/indagato* che per la (diversa) *persona interessata al prelievo,* esplicitamente intendendo che l'accertamento possa non riguardare solo chi sia sottoposto alle indagini, e prevedendolo, se necessario, anche per altre persone, pur non indagate.
In tale ultima ipotesi tuttavia la procedura di prelievo coattivo può giustificarsi solo con l'assoluta indispensabilità dell'adempimento. L'esistenza in capo al prossimo congiunto dell'indagato di una serie di diritti e facoltà per la tutela del vincolo familiare induce comunque ad escludere quello coatto nei confronti di questi (cd. familial searching). L'art. 392, c. 2 cpp (art. 28) in tema di incidente probatorio prevede l'uso di tale strumento di anticipazione nella raccolta della prova. **Per quanto concerne l'attività d'iniziativa della PG**, gli articoli 133 e 354 cpp (artt. 26 e 27 L. n. 85/2009) contemplano e disciplinano il prelevamento, anche coattivo di capelli, peli, saliva etc, in mancanza quindi del consenso (art. 349, c. 2 bis cpp), nell'ambito dell'identificazione svolta dalla PG, con la necessaria autorizzazione del PM. Il prelievo viene effettuato dai campioni di mucosa orale ad opera di operatori della Polizia Penitenziaria specificamente addestrati, o delle FFPP, possibilmente sulla scena del crimine nel rispetto della dignità e della riservatezza delle persone. Il campione prelevato deve essere immediatamente inviato, al Laboratorio centrale, per la tipizzazione del relativo profilo e la successiva trasmissione alla BDN - DNA.
L'accesso alla BDN - DNA, per la consultazione, si configura di secondo livello, con la completa identificazione dell'operatore e la sua registrazione (in un file di log) per ogni attività svolta, sia sui profili che sui campioni. Come modalità procedurale per l'acquisizione del nome della persona cui appartiene il profilo, è previsto che la PG e la stessa AG debbano preventivamente richiedere il confronto e, solo in caso positivo, possono essere autorizzate ad acquisirne le generalità. **Il consenso per il prelievo di campiono biologici su minori** e su persone incapaci o interdette è disciplinato dall'art. 72 bis delle norme di attuazione cpp (art. 29 L. cit).
Alcuni reati c.d. dei colletti bianchi (tributari in primis, ma anche contro la P.A.) sfuggono alla raccolta del DNA ed il riferimento è all'art. 9 della citata L. n. 85/2009.

NOTA ESPLICATIVA

I rilievi segnaletici (fotosegnalamento) consentono di acquisire **dati biometrici** attraverso un trattamento tecnico specifico e sono relativi alle caratteristiche fisiche, consentendo o confermando l'identificazione univoca di una persona fisica. Sono descrittivi (caratteristiche somatiche del soggetto), fotografici (immagine fotografica della persona) e dattiloscopici (prelievo delle impronte delle falangi delle dita e dei palmi delle mani). Vengono riassunti in un'apposita scheda su modello conforme a quello elaborato dal Ministero dell'Interno nell'ambito del citato **AFIS**: sistema automatizzato per l'identificazione delle impronte digitali del casellario centrale d'identità. In pratica consiste nella registrazione di tali rilievi, effettuati mediante l'evidenziazione di caratteristiche somatiche già prefigurate nella scheda; viene poi fotografato il volto della persona ed il suo profilo destro, con l'orecchio scoperto, rappresentando anche l'orecchio medesimo un elemento di identificazione comparabile per la ricerca dell'identità. Nel caso sul profilo sinistro del soggetto si rilevassero particolari segni, utili per la sua identificazione, viene fotografato anche il profilo sinistro. Nel caso di rifiuto (o di fondato sospetto che la persona abbia fornito false generalità), a norma dell'art. 11 della legge 191/1978, oppure (se l'identificazione avviene ai fini giudiziari) a norma dell'art. 349 cpp, si può procedere all'accompagnamento per l'identificazione. Se la persona non aderisce spontaneamente all'invito di seguire gli agenti presso l'ufficio di polizia, si procede all'accompagnamento coattivo. Nell'ambito di un accertamento sulle generalità può assumere rilievo il fatto che eventuali induzioni in errore circa dati personali identificativi, o qualifiche o qualità cui la legge attribuisca effetti giuridici, declinate dal soggetto siano state finalizzate ad ottenere un vantaggio per sè o per altri ovvero a procurare ad altri un danno integrando anche il delitto di *sostituzione di persona* (art. 494 c.p.). Per tale fattispecie rileva anche la dichiarazione fatta ad un privato e non necessariamente solo al pubblico ufficiale (Cass., Sez. 5, 28 novembre 2012, n. 18826) La S.C. ritiene inclusi gli pseudonimi cibernetici, tipicamente i

nickname, tra i contrassegni identitari utilizzabili per attribuire *"a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici"*. Il fatto deve essere tuttavia strettamente correlato all'utilità prospettata per l'autore, ovvero all'attività molesta posta in essere dal reo per arrecare a terzi un danno o un disturbo rilevante da valutarsi alla stregua di un *Disturbo alle persone* (art. 660 cp). Qualora l'inganno circa i titoli gli onori e le qualifiche posseduti sia derivato dal possesso di segni distintivi contraffatti (art. 497- ter c.p. - *Possesso di segni distintivi contraffatti*) o dal fatto di aver portato in pubblico divise segni distintivi o abiti ecclesiastici (art. 498 c.p. - *Usurpazione di titoli e di onori*). Un eventuale abuso può configurare *Interferenze illecite nella vita privata* (art. 615 bis cp), col procurarsi indebitamente notizie o immagini attinenti alla vita privata con l'uso di strumenti di ripresa visiva o sonora.

Il Sistema Periferico di Acquisizione delle Impronte Digitali (SPAID) viene utilizzato dalle FFPP, consentendo l'identificazione delle persone attraverso l'acquisizione e il riconoscimento delle loro impronte digitali. Consente l'acquisizione a livello locale delle impronte, della foto, dei segni particolari e dei dati anagrafici, effettua, tramite algoritmi, l'estrazione delle caratteristiche dell'impronta, la compressione dei dati e il loro invio criptato al sistema centrale AFIS. Da un punto di vista tecnico integra un PC portatile dotato di modem e scheda LAN, con uno scanner per l'acquisizione delle impronte digitali e una videocamera. Può così essere impiegato praticamente in ogni luogo ove si renda necessario procedere all'identificazione di persone. Il collegamento alla banca dati AFIS può avvenire via telefonica RTG, rete IP o GPRS/GSM. Il procedimento di identificazione restituisce il Codice Unico di Identificazione (CUI) della persona e gli eventuali precedenti fotosegnalamenti. Il CUI è correlato al *dato biometrico*, assunto quale *criterio di identificazione univoca*.

09)Dealer - fornitore servizi di connettività.

Rileva l'identificazione fatta da privati quando venga consegnata o messa a disposizione una SIM (*Subscriber's Identity Module*), che non deve essere considerata un servizio venduto al cliente, bensì alla stregua di un bene materiale (supporto), strumentale all'identificazione di chi usufruisce del servizio di telefonia o connettività. Prima dell'attivazione, quando viene consegnata o messa a disposizione, il *Dealer* deve acquisire i dati anagrafici attraverso una corretta identificazione (*Codice delle Comunicazioni Elettroniche*) da ritenersi effettuata nell'ambito della c.d. *data retention*. L'A. G. può accedere per fini di giustizia agli elenchi - utenti che devono essere trasmessi al CED del Ministero dell'interno.

Le disposizioni antiterrorismo (D.L. 27 luglio 2005 n. 144 conv. L. n. 155 del 31 luglio 2005), prevedono che anche le carte preattive non possano funzionare fino al caricamento dei dati anagrafici dell'acquirente. È tuttavia possibile (D.L. 18 ottobre 2012 n. 179), per le SIM abilitate al solo traffico dati, identificare e registrare gli utenti anche in via indiretta, attraverso sistemi di riconoscimento via SMS e carte di pagamento nominative. Ciò presuppone un'identificazione vera e propria già effettuata per altri motivi (per le carte di pagamento nominative, vds. antiriciclaggio. Resta irrisolto il problema di fondo, la sempre possibile mancata corrispondenza tra intestatario della SIM e suo effettivo utilizzatore.

10)L'identificazione di polizia economica e finanziaria

L'identificazione di persone fisiche ma anche soggetti diversi, assume determinante rilievo, nelle indagini sui reati finanziari, ma anche per il riciclaggio, i reati fallimentari o economici in genere e per aggredire patrimoni illeciti. La legge antiriciclaggio (d.lgs. 231/2007 agg. d.lgs. 90/2017, di seguito LA) compendia i diversi adempimenti cui fa riferimento la normativa di settore. Malgrado possa ritenersi univocamente identificato un soggetto per il quale si disponga di dati personali che consentano, come la Partita I.V.A. o il C.F., la certa riferibilità, la necessità di notificare atti o eseguire controlli rende sempre indispensabile completare la procedura di identificazione. L'identificazione di Polizia Tributaria, rectius di Polizia Economica e Finanziaria, presenta delle particolarità sia relativamente alle persone fisiche che ai soggetti diversi da queste. **Un contribuente** può essere identificato, dall'Agenzia delle Entrate e dalla G.d.F., attraverso la Dichiarazione delle persone fisiche (art.38 del D.P.R. 600/73), ovvero attraverso la Dichiarazione dei soggetti diversi dalle persone fisiche (art.40 del D.P.R. 600/73). **Gli evasori totali** sfuggono evidentemente a tale possibilità e vengono individuati e identificati attraverso controlli e ricerche (art. 37, c.2, del D.P.R. 600/73). **I soggetti non residenti nello Stato**, esercenti attività d'impresa, arte o professione in altro stato U.E. o in paese terzo, rispetto al quale vi siano strumenti giuridici che prevedano la reciproca assistenza in materia di imposizione indiretta, che intendano porre in essere operazioni rilevanti ai fini IVA, assolvendone gli obblighi ed

esercitandone i diritti, in particolare quello di detrazione sugli acquisti effettuati nel territorio italiano, evitando la procedura del rimborso, in alternativa alla nomina di un rappresentante fiscale, possono identificarsi direttamente (art. 35 ter L. 633/72). Tale identificazione rende possibile far confluire nella posizione IVA attribuita alla **stabile organizzazione** tutte le operazioni. **Il domicilio fiscale** viene determinato, per l'applicazione delle imposte sui redditi, secondo le regole di cui all'art. 58 del D.P.R. 600/73, sia per le persone fisiche che per i soggetti diversi dalle persone fisiche. Costituisce un elemento importante per l'identificazione dei soggetti. Un aspetto strettamente connesso è costituito dalla **residenza fiscale** che esplica un effetto sostanziale in ordine alla tassazione in Italia dei redditi prodotti. Il criterio per l'attribuzione della residenza è rinvenibile nell'art. 2 del T.U.I.R. (DPR 22 dicembre 1986, n. 917).
Rileva a tal proposito la volontà di fissare in un determinato luogo il centro delle proprie relazioni economiche e personali. L'iscrizione anagrafica tra la popolazione residente rappresenta un caso di presunzione assoluta di residenza fiscale nel territorio dello Stato. L'iscrizione all'AIRE non determina invece automaticamente la cessazione della residenza fiscale in Italia, ben potendo la stessa ricavarsi dall'applicazione delle altre regole stabilite dal citato art. 2 T.U.I.R. Tali si sostanziano nel domicilio e nella residenza in Italia secondo il codice civile. Si considerano (anche se non lo sono) altresì fiscalmente residenti, salvo prova contraria, i cittadini italiani cancellati dalle Anagrafi della popolazione residente ed emigrati in Stati o territori aventi un regime fiscale privilegiato, individuati con decreto del Ministro delle Finanze. Discende implicitamente dalla obbligatorietà del rilascio della ricevuta fiscale, la necessità di identificare il cessionario o committente (art. 2 c. 2, D.M. 2 lug. 1980) di un'operazione documentata. Altrettanto è previsto per il destinatario dello scontrino fiscale (art. 2, L. 26 gen. 1983, n.18) ancorché non sia più destinatario di sanzioni.
Codice Fiscale (CF) e Partita IVA (PI), intesi con l'acronimo **T.I.N.** (*Tax Identification Number*) nelle convenzioni internazionali, consentono una precisa individuazione di soggetti, persone fisiche e non, nella rilevazione dati. I paesi O.C.S.E. attribuiscono un T.I.N. ai propri contribuenti. Sono dati personali che assumono rilevanza solo con la procedura di attribuzione ma rappresentano una chiave per i programmi automatizzati di controllo incrociato. La conoscenza del TIN è necessaria, in particolare nel trattamento delle informazioni ricevute in via automatica da uno Stato membro" (Manuale O.C.S.E.). L'obbligo di indicare il C.F. da parte di persone fisiche e giuridiche (art. 1, c. 222, l. 24/12/2007, n. 244) risulta esteso ai contratti di telefonia fissa, mobile e satellitare, con indubbia efficacia in termini di identificazione. Il TIN è quindi il principale elemento identificativo del contribuente e dei cittadini in genere nonché di persone fisiche e soggetti diversi non residenti nei rapporti con operatori finanziari nazionali. In materia antiriciclaggio C.F. e P.I. sono essenziali per identificare i vari soggetti.
Il C.F. per le persone fisiche è composto da un'espressione alfanumerica di sedici (16) segni di cui: • prima, seconda e terza consonante del cognome e se non bastano le prime vocali, se ancora non bastano si aggiunge una X; • prima, terza e quarta consonante del nome e, se non bastano, le prime vocali, se ancora non bastano si aggiunge una X; • le ultime due cifre dell'anno di nascita; • una lettera che rappresenta il mese di nascita; • due cifre per il giorno di nascita e per il sesso, per i maschi si tratta del giorno effettivo, per le femmine si aggiunge 40; • tre segni, secondo una tabella prefissata, per il comune italiano di nascita o stato estero; • un carattere alfabetico di controllo che scaturisce da apposita procedura di calcolo prestabilita. La possibilità di una pressoché certa identificazione dei soggetti può essere di grande importanza. Tenendo tuttavia presente che il C.F. non scongiura i casi, rarissimi, di omonimia estesa anche a quest'ultimo. Tale situazione, detta di omocodia, viene risolta dall'Agenzia delle Entrate attribuendo al soggetto un C.F. diverso da quello che discenderebbe dalle suddette regole generali di formazione. Ciò avviene attraverso la sostituzione di una o più cifre, a partire da quella più a destra, con corrispondenti caratteri alfabetici. Sul sito dell'Agenzia è disponibile il software per la verifica del C.F.
Il C.F. per i soggetti diversi dalle persone fisiche è composto da un'espressione numerica di undici (11) cifre e corrisponde al numero di partita I.V.A. (attribuita a soggetti residenti, stabili organizzazioni in Italia o rappresentanti fiscali di soggetti non residenti, ovvero soggetti non residenti che provvedono direttamente agli adempimenti IVA) per cui non è possibile l'omonimia. In ambito U.E. il sistema informativo VIES (*Vat*

Information Exchange System) consente, anche ai privati, di accedere per ottenere conferma della validità del numero di identificazione I.V.A. di un soggetto.

Il codice EORI (*Economic Operator Registration and Identification*), alfanumerico univoco, serve per la registrazione e l'identificazione degli operatori economici e degli altri soggetti in ambito doganale (U.E.), in caso di: importazioni, esportazioni, circolazione merci in regime di transito, autorizzazioni per fruire di semplificazioni doganali o regimi doganali. L'attribuzione è automatica per tutti i soggetti nazionali (speditori, esportatori, importatori, importatori, obbligati principali) che abbiano effettuato operazioni doganali. Per i titolari di partita IVA, corrisponde alla stessa preceduta dalle lettere IT. Per i soggetti non titolari di partita IVA e diversi da persona fisica, viene attribuito un codice IT seguito dagli undici caratteri del codice fiscale. Per gli altri soggetti persone fisiche dal codice IT e dal C.F. senza l'ultimo carattere.

Il codice CUAA (*Codice di Identificazione delle Aziende Agricole*) identifica gli imprenditori agricoli nei loro rapporti con la Pubblica Amministrazione e corrisponde al codice fiscale (art. 1, c. 2, D.P.R. 503/99).

Lo status di Certified Taxable Person (CTP), - proposta della Commissione EU-COM (2017) n. 566 - riferibile alla riforma del regime transitorio IVA (UE), identificherebbe soggetti passivi ritenuti fiscalmente affidabili per cui far sopravvivere la regola dell'esenzione, risultando equivalente a quello di **Authorised Economic Operator** (AEO) in ambito doganale. Avendo come obiettivo la tassazione delle operazioni transnazionali nello Stato di origine, ma con le aliquote del Paese di destino, il progetto prevede l'utilizzo del *One Stop Shop*, già operativo per i servizi digitali. I CTP resterebbero gli unici soggetti a beneficiare della regola dell'esenzione.

11)L'identificazione nell'Antiriciclaggio e nel contrasto del finanziamento del terrorismo

L'adeguata verifica della clientela può intendersi **modalità d'identificazione particolarmente approfondita** (rafforzata ex art. 24, semplificata ex art. 23 LA), nei confronti di chi instauri un rapporto continuativo, ovvero una prestazione professionale a seguito di conferimento di incarico, o a fronte di un'operazione occasionale che comporti movimentazione di mezzi di pagamento (euro o valuta) pari o superiori a 15.000 euro attraverso operazioni collegate che realizzino un'unica operazione frazionata. Viene in considerazione anche un singolo trasferimento di fondi superiore a 1000 euro, dovendo i dati accompagnare i trasferimenti in qualsiasi valuta, relativamente all'ordinante e al beneficiario nel caso uno dei prestatori di servizi di pagamento coinvolti nel trasferimento sia stabilito nell'U.E. Sono esonerati dall'adeguata verifica i professionisti, principalmente gli avvocati, prima che sia loro conferito l'incarico (attività forensiche) di difesa e rappresentanza in giudizio in senso lato, inclusa la consulenza volta ad intraprendere od evitare un giudizio, fermo restando gli obblighi di identificazione (art. 18 n. 4 LA). Dando presupposta la presenza fisica del cliente o di un esecutore persona fisica (delegato in nome e per conto di questi), viene identificato, anche in ordine all'esistenza e all'ampiezza del potere di rappresentanza (art. 18 c. 1 a LA), accertando il titolare effettivo dell'operazione o rapporto (art. 19 LA). I dati identificativi (art. 1 c. 2, n LA) sono quelli contenuti nella C.I. (o documenti di riconoscimento equipollenti), inclusi residenza anagrafica e domicilio ove quest'ultimo non fosse coincidente, il TIN (C.F. o la P.I.) la denominazione e la sede legale. Determinare esistenza e ampiezza del potere di rappresentanza può non essere agevole, ma il cliente e l'esecutore dell'operazione sono tenuti a fornire le relative informazioni, altrimenti da ricercarsi attraverso fonti affidabili e indipendenti.

La persona fisica presente viene identificata attraverso C.I. (o doc. equipollente), in corso di validità (DPR n. 445/2000) da acquisire in copia (formato cartaceo o elettronico ex art. 19 c. 1 a LA) e C.F. Resta salva la possibilità di un'identificazione attraverso un'identità digitale di livello massimo di sicurezza di cui al CAD (Codice dell'Amministrazione digitale - D.lgs. n. 82 del 2005) o certificato di firma digitale compreso nell'elenco pubblicato dalla Commissione Europea (Reg. UE n. 910/2014). I soggetti che esercitano il gioco on line devono effettuare l'identificazione della clientela e la relativa verifica (art. 53, c. 1, LA), in occasione dell'apertura o modifica di un conto di gioco (di cui all'art. 24, L. n. 88/2009). Nelle case da gioco (casinò a controllo pubblico) è necessaria la previa identificazione e verifica della clientela sin dal suo ingresso (art. 53, c. 11, LA), per correlare ogni operazione di gioco ad un ben individuato cliente.

L'identificazione indiretta di un cliente si rende possibile pur senza la sua presenza, quando sia già stato identificato dallo stesso operatore finanziario o professionista, purchè le informazioni risultino aggiornate ed adeguate per il previsto profilo di rischio, ovvero quando i suoi dati identificativi risultino da atti ritenuti idonei dalle Autorità di Vigilanza di settore (art. 19, 6 LA), o risultino da dichiarazione dell'autorità consolare italiana (d.lgs. 153/1997). L'identificazione può risultare, da attestazione di altro intermediario bancario o finanziario, professionista o società di revisione di un Paese UE. In tale modalità si ricomprendono anche le operazioni effettuate con sistemi di cassa continua, presso gli sportelli automatici, per corrispondenza o mediante carte di pagamento; tali operazioni sono imputate al titolare del rapporto al quale ineriscono. L'identificazione a distanza è accettabile senza la presenza fisica delle controparti, ove il cliente sia in possesso, a seguito di avvenuta identificazione personale, di un'attestazione di un intermediario abilitato o di un ente creditizio o finanziario di Paese U.E. o aderente al GAFI; nell'ipotesi di Paesi extra-UE o non appartenenti al GAFI, l'identificazione è tuttavia valida se operata da una banca succursale in tali Paesi di banche di paesi U.E. o GAFI.

La titolarità effettiva per clienti diversi dalle persone fisiche (art. 20 LA) viene determinata prendendo in considerazione le persone cui sia da attribuire la proprietà diretta o indiretta dell'ente. Per le società di capitali, tale criterio si ritiene soddisfatto con una percentuale di partecipazione al capitale sociale, ottenuta anche attraverso altro soggetto giuridico, superiore al 25%, quando vi sia il controllo sulla maggioranza dei voti esercitabili nell'assemblea, ovvero quando tale controllo sia sufficiente ad esercitarvi un'influenza dominante anche attraverso vincoli contrattuali. Per i trust e soggetti giuridici analoghi, viene richiamata l'adozione di misure adeguate e commisurate alla situazione di rischio per comprendere la struttura di proprietà e di controllo. Per facilitare la decodifica di strutture complesse d'ingegneria finanziaria, utilizzate per schermare la provenienza di capitali, viene prevista l'alimentazione, unicamente attraverso modalità telematiche, con i dati previsti e che erano fino ad ora ritenuti riservati, di un apposito "*Registro dei titolari effettivi delle persone giuridiche e trust espressi*". La sua consultazione è consentita, attraverso una sezione riservata del "*Registro delle imprese*", al MEF, alle autorità di vigilanza di settore, all'UIF, alla DIA, alla G.d.F. quando opera in materia di antiriciclaggio attraverso il N.S.P.V., alla DNAA, all'A.G., all'autorità fiscale, ma anche ai "soggetti obbligati", previo accreditamento, come pure e con modalità analoghe ai soggetti privati, anche portatori di interessi diffusi per la tutela di situazioni giuridicamente rilevanti (art. 20, c° 2, LA). L'accesso a tali informazioni può essere escluso qualora riguardi persone incapaci o minori, ovvero esponga il titolare effettivo a rischi per la propria incolumità. Possono così essere acquisite informazioni aventi valore di atti pubblici fidefacenti, circa la titolarità effettiva, non solo di società, gruppi di società ed enti diversi, ma, cosa più importante, circa trust produttivi di effetti fiscali, che giovano ad una migliore conoscenza complessiva della propria clientela da parte dei soggetti obbligati. Viene così resa possibile l'individuazione del c.d. *beneficial owner*, con le società e le altre entità giuridiche tenute ad acquisire *informazioni adeguate e aggiornate*, sulla propria titolarità effettiva, con obbligo di conservazione in registri centrali.

Tutti i cittadini U.E. e le persone giuridiche dovranno essere resi identificabili in relazione al possesso di conti bancari e di pagamento entro il 10 gennaio 2020 (recepimento) nell'intero ambito dell'Unione, direttiva (U.E.) n. 2018/843 (art. 32 bis): *Gli Stati membri istituiscono meccanismi centralizzati automatici, quali registri centrali o sistemi elettronici centrali di reperimento dei dati, che consentano l'identificazione tempestiva di qualsiasi persona fisica o giuridica che detenga o controlli conti di pagamento, conti bancari identificati dall'IBAN, come definito dal regolamento (UE) n. 260/2012 del Parlamento europeo e del Consiglio e cassette di sicurezza detenuti da un ente creditizio nel loro territorio. Gli Stati membri notificano alla Commissione le caratteristiche di detti meccanismi nazionali*. …

In merito ai detentori di beni immobili: *Gli Stati membri* (entro il 10 gennaio 2020 recepimento) *forniscono alle FIU e alle autorità competenti l'accesso alle informazioni che consentono l'identificazione tempestiva di qualsiasi persona fisica o giuridica che detenga beni immobili, anche attraverso registri o sistemi elettronici di reperimento dei dati, se disponibili*. - direttiva (U.E.) n. 2018/843 (art. 32 ter).

Non ha la qualifica di pubblico ufficiale l'incaricato, che esegua gli adempimenti assegnati dall'obbligato (LA) e non può quindi avvalersi, per l'identificazione di un documento scaduto di validità. Acquisisce e valuta

informazioni dal cliente, tenuto a fornirle, circa la propria persona e lo scopo dell'operazione. Può avvalersi di banche dati accessibili tra cui il sistema pubblico per la prevenzione del furto di identità (D.lgs. n. 64/2011).
Fattispecie incriminatrici sono previste per la clientela che fornisca dati e informazioni non veritiere (art. 55 *sanzioni penali*, LA), ovvero per coloro che, tenuti alla verifica, non svolgano dolosamente in maniera efficace il compito, falsificando dati e informazioni (art. 55, 1 LA), acquisendoli o conservandoli nella consapevolezza della loro falsità (art. 55, 2 LA). Risultano inoltre perseguibili i soggetti terzi che, obbligati dalla LA, forniscano dati falsi o informazioni non veritiere ai soggetti obbligati alla verifica (art. 55, 3 LA).
Inapplicabili risultano invece le ordinarie fattispecie di reato per il rifiuto e le false generalità per l'assenza della qualifica di P.U. da parte di chi viene chiamato a svolgere le formalità dell'identificazione.

12)I dati personali delle persone fisiche nell'attività di polizia

(*General Data Protection Regulation,* Reg. (UE) 2016/679 – GDPR - e D.lgs. n. 51 del 18/mag./2018)

La disciplina del trattamento dei dati personali per finalità di polizia e più in generale in materia di indagini, è rinvenibile principalmente nel *General Data Protection Regulation*, Reg. (UE) 2016/679 – GDPR e nel D.lgs. n. 51 del 18/mag./2018). Risulta però tuttora non esplicitamente abrogato il Codice in materia di protezione dei dati personali o *Codice della Privacy* (D.lgs 196/2003), che è tuttavia solo parzialmente compatibile col citato Regolamento 679/2016 (GDPR). Prevalendo ovviamente quest'ultimo sulla legge nazionale, s'intende l'automatica abrogazione del codice, ove in contrasto, e quando regoli la stessa materia, per disapplicazione; il D.lgs. 196/2003 subisce in effetti una rilettura, da farsi anche considerando i collegati D.M. Interno 24 maggio 2017 e il DPR n. 15/2018, concernente: trattamenti effettuati per finalità di polizia, in modalità elettronica, e in forma cartacea. Il *Codice della privacy* all'art. 53, c.1, intende effettuati per tale finalità i trattamenti: … direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati. Analogamente trova fondamento nella nuova Legge (art. 5 D.lgs. cit.) che autorizza, nel trattamento dei dati personali, una base giuridica diversa dal consenso dell'interessato. La protezione dei dati delle persone fisiche, nell'ambito dell'investigazione/penale (prevenzione, indagine, accertamento e perseguimento di reati, oltre che dell'esecuzione penale) viene delineata compiutamente, sotto il profilo della privacy, dal cit. D.lgs. n. 51 del 18/mag./2018 (art.1) attuativo del GDPR, quando disciplina le modalità del trattamento anche solo parzialmente automatizzato e di quello non automatizzato dei dati contenuti o destinati ad un archivio. Risulta a tale riguardo una sovrapposizione col testo del codice della Privacy (art. 11), derivandone i requisiti di esattezza, aggiornamento, pertinenza, completezza e non eccedenza rispetto alle evocate finalità. Quindi i relativi programmi informatici devono risultare configurati soddisfacendo le necessità operative, ma riducendo, ove possibile al minimo, l'utilizzo di dati personali, consentendone la cancellazione o l'anonimizzazione con modalità automatizzate allo scadere dei termini di conservazione e quando abbiano esaurito la propria finalità; gli accessi e le operazioni effettuati, solo da operatori abilitati, devono inoltre essere registrati in appositi file di log.
La raccolta ed il trattamento dei dati personali (art. 11 del DPR 15/2018), risultano vietati in senso assoluto se motivati unicamente dalla volontà di una schedatura circa: origine razziale o etnica delle persone, fede religiosa, opinione politica, orientamento sessuale, salute, convinzioni filosofiche o di altro genere o l'adesione ai principi di movimenti sindacali, nonché l'attività legittima svolta come appartenenti ad organizzazioni operanti negli stessi settori; potendo invece configurarsi la liceità di un tale trattamento, qualora si renda necessario per le esigenze di un'attività informativa, di sicurezza o di indagine di polizia giudiziaria o di tutela dell'ordine e della sicurezza, ad integrazione di altri dati personali, per contrastare crimini come il terrorismo. La disciplina della comunicazione dei dati personali verso soggetti terzi (DPR 15/2018) risulta diversificata a seconda del destinatario:
- **tra le FFPP** (art. 16 L. n. 121/1981) per finalità istituzionali è ammessa, fermo restando gli obblighi di riservatezza propri dell'ambito investigativo;

Il Capo III della legge 85/2009 disciplina:
- **nell'ambito dello scambio di informazioni previsto da trattati internazionali**, tra Stati aderenti, es quello di Prüm sul DNA (art. 20 L. n. 85 /2009), è ammessa nel rispetto delle modalità di volta in volta stabilite;
- **verso le altre P.A.** o enti pubblici, è consentita solo nei casi previsti da disposizioni di legge o di regolamento o quando si renda necessaria per uno specifico compito istituzionale dell'organo di polizia e i dati da trasmettere siano necessari per i compiti pure istituzionali del ricevente (art. 13, c. 1, DPR 15/2018), nel rispetto del segreto investigativo e d'ufficio;
- **verso i privati**, è consentita quando risulti necessaria per adempiere uno specifico compito istituzionale da parte dell'organo (ufficio o comando) per le finalità polizia;
- **ben diversa da quella di comunicazione si configura la stessa nozione di diffusione** (a mezzo WEB, TV, media etc.) di tali dati (art. 14, DPR 15/2018), per la indeterminatezza dei destinatari, venendo contemplata e consentita per soddisfare finalità di polizia (art. 3), ma comunque nel rispetto del segreto di indagine e fatti salvi i limiti specifici derivanti da leggi o di regolamenti; particolari risultano le condizioni richieste per la diffusione di immagini personali, ammessa solo col consenso dell'interessato o se necessaria per salvaguardare la vita o l'incolumità fisica, al limite per stringenti necessità di giustizia o polizia.
Analoga rigorosa disciplina non risulta automaticamente applicabile ai analoghi trattamenti effettuati per finalità di sicurezza nazionale e salvaguardia dei principi democratici dell'UE: interesse economico o finanziario dell'Unione o di un membro (moneta, bilancio, sanità pubblica e sicurezza sociale, indipendenza della magistratura), da parte di istituzioni, organi, uffici e agenzie UE (titolo V, capo 2, TUE).
Ciò detto dato personale (art. 2 c.1 lett. a D.lgs. cit.) deve intendersi lo strumento tecnico-giuridico che consenta di giungere all'identificazione di una persona fisica. Per persone diverse da quelle fisiche non può parlarsi di dato personale, venendo semmai in considerazione per tali soggetti il diritto al rispetto del domicilio ovvero della corrispondenza. Il diritto UE non prevede, per quel che ci occupa, la tutela dei dati delle persone giuridiche. Pseudonimizzazione (lett. d) s'intende un trattamento che consenta la non ulteriore attribuzione di dati personali ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, che siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che non possano essere attribuiti a una persona identificata o identificabile. Interessato è una persona fisica cui si riferiscano i dati oggetto di trattamento (art. 4, par. 1, p. 1 GDPR). Titolare è una persona fisica, un'autorità pubblica, un'impresa, un ente, un'associazione, che adotti o decida un trattamento e relative modalità (art. 4, parag. 1, p. 7 GDPR). Responsabile è una persona, fisica o giuridica, cui il titolare affidi, anche esternalizzando, specifici e definiti compiti di gestione, controllo e trattamento dei dati personali per suo conto, fatta salva la possibilità di designare un altro soggetto sub-responsabile. Pur essendo temi strettamente correlati viene escluso ogni riferimento alla *Cyber security*, il cui ambito (non solo tecnico) prevede la non accessibilità dei dati da parte dei non autorizzati, prescindendo dalla loro riferibilità ad una persona fisica, piuttosto che ad un'azienda o ad una pubblica amministrazione, sovrapponendosi invece alla Data Protection con riferimento alla correttezza nella gestione del dato, alla sua non eccedenza ai fini di un trattamento, alla conservazione e alla riservatezza. Non esiste, nella gestione della privacy, una formale distinzione soggettiva tra obbligati che siano pubblici o privati, ma nel cit. D.lgs. n. 51 del 18/mag./2018, per il settore che ci occupa, si prevede una riserva nel trattamento dei dati giudiziari (art. 10 del GDPR) che può avvenire sotto il controllo di un'Autorità pubblica, mentre negli altri casi deve essere consentito dalla Legge. Altrimenti determinante per la liceità di qualsiasi trattamento dei dati risulta la specifica finalità (base giuridica) per cui avviene, a prescindere dalle qualifiche di chi lo effettui (art. 6, lett. e GDPR). Le informazioni si considerano tali in quanto riconducibili, attraverso un'identificazione diretta a persone fisiche, o quando risultino comunque idonee per quella indiretta attraverso elaborazioni o ricerche, con riferimento alle Tecnologie dell'Informazione e della Comunicazione (I.C.T. Information and Communications Technology) rilevando peraltro nella categoria dei dati personali anche quelle riferibili alle comunicazioni elettroniche e alla geolocalizzazione. Sono ritenute idonee ad identificare direttamente l'interessato le informazioni definite con l'acronimo PII (Personally identifiable information), tali definite dal NIST (Istituto nazionale degli standard e della tecnologia): nome e cognome, indirizzo di casa, e-mail, numero identificativo nazionale (TIN, in Italia C.F. e P.I.), numero di

passaporto, indirizzo IP (se collegato ad altri dati), numero di targa di un veicolo, numero di patente, volto, impronte digitali o calligrafia, numeri di carta di credito, identità digitale, data di nascita, luogo di nascita, numero di telefono, account name o nickname e dati genetici. Possono risultare descrittivi di una persona al punto di consentirne l'identificazione, anche ricorrendo a dati ulteriori, quelli genetici o biometrici, che includono le fotografie caricate on-line, venendo impiegati correntemente per identificare i passeggeri in taluni aeroporti, o per consentire la fruizione di particolari servizi bancari e da ultimo per l'accesso a profili social. Il GDPR disciplina con maggior rigore il trattamento dei dati particolari, precedentemente definiti sensibili (condizioni di liceità: artt. 6 e 9 c. 2). Tali (art. 9, 51 e 56 Reg.) devono essere intesi: origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche; appartenenza sindacale, genetici, biometrici a scopo identificativo, salute, vita e orientamento sessuale. Il Garante ha fornito (materia sanitaria) indicazioni, per un'interpretazione uniforme, utili anche per l'argomento dell'identificazione che ci occupa. … "I medici potranno trattare i dati dei pazienti, per finalità di cura, senza dover richiedere il loro consenso, ma dovranno comunque fornire loro informazioni complete sull'uso dei dati. … omissis … Tutti gli operatori del settore dovranno tenere un registro dei trattamenti dei dati. … il professionista sanitario, soggetto al segreto professionale, non deve più richiedere il consenso per i trattamenti di dati necessari alla prestazione sanitaria." È invece richiesto il consenso, o una differente base giuridica, quando tali trattamenti non sono strettamente necessari per le finalità di cura, anche quando sono effettuati da professionisti della sanità. … omissis … è obbligatorio per tutti gli operatori sanitari tenere un registro nel quale sono elencate le attività di trattamento effettuate sui dati dei pazienti (in cui riportare le richieste dell'Autorità ndr.). Tale documento rappresenta, in ogni caso, un elemento essenziale per il "governo dei trattamenti" e per l'efficace individuazione di quelli a maggior rischio, anche per dimostrare il rispetto del principio di responsabilizzazione (accountability) previsto da GDPR. Il trattamento finalizzato alle indagini (rectius relativi a reati e misure di sicurezza art. 6, par. 1, Reg.), sotto il controllo dell'Autorità pubblica, è ovviamente consentito (art. 10 Reg.), fuori da tale controllo quando autorizzato dalla legge e prevedendo garanzie appropriate per i diritti e le libertà degli interessati" (art. 2-octies, c. 1, d.lgs. 101/2018). La regola che vieta il trattamento di tali famiglie di dati ha quindi un valore di mera enunciazione, prevedendosi le deroghe che la Legge stessa indica e che l'intelligenza presuppone, ad es.: ipotesi che i dati siano già manifestamente pubblici (o resi tali ad opera degli stessi soggetti), consenso esplicito, esistenza di una base giuridica (Legge o altra) che lo preveda per le cennate finalità pubbliche di sicurezza e giustizia (o sanità pubblica, …). Il trattamento che avvenga su base consensuale presuppone un termine nella conservazione dei dati, per cui si rende necessario renderlo noto, mentre alla scadenza vanno anonimizzati o cancellati, salvo che non possa ritenersi successivamente applicabile una base giuridica diversa, come nell'adempimento di obblighi antiriciclaggio e fiscali o perché divengano necessari per tutelare legittimi interessi del titolare del trattamento; un caso di specie potendo ravvisarsi nella documentazione relativa ad un rapporto di conto corrente bancario, di durata indeterminata, da conservarsi per dieci anni oltre la data di estinzione. Durate la delicata fase iniziale della loro acquisizione dall'interessato, da parte degli obbligati, rileva pertanto la necessità di fornire informazioni che garantiscano un consenso informato (art. 4 GDPR), relativamente alla manifestazione di volontà della persona fisica che sia capace di agire, almeno sedicenne (cc art. 1), altrimenti dell'esercente la potestà dei genitori. Tale deve essere: libera (art. 7 GDPR), la figura del datore di lavoro ad es. risultando in qualche misura ostativa rispetto all'ipotesi di un consenso spontaneamente reso dal dipendente, ove sia ravvisabile un pregiudizio, a causa della supremazia sullo stesso che rende necessario opinare per un trattamento dei dati che presupponga una diversa base giuridica; specifica (art. 32 GDPR), cd granularità del consenso, richiesto specificamente per ogni trattamento nell'ipotesi di plurime finalità; informata (art. 4 GDPR), garantendosi una sintetica conoscenza dei diritti, consapevolezza dei dati utilizzati, insieme a modalità e finalità del trattamento, conseguenze del consenso; verificabile pur non necessariamente da documentarsi per iscritto, salvo la necessità di dimostrarlo con riferimento ad uno specifico trattamento che va distintamente indicato, sempre dovendo risultare il titolare in grado di riferire a quale informativa l'interessato abbia prestato il proprio consenso; revocabile con la stessa facilità, senza obbligo di motivazione, mentre, dovendo interrompersi il trattamento, ciò non implica l'illiceità di quello già posto in essere, ma solo

la doverosità di cessarlo, se non vi sia la possibilità/necessità di proseguirlo su una differente base giuridica; inequivocabile, caratteristica che può far sorgere qualche dubbio, unambiguous recitando infatti il testo originale, ed il termine non è esattamente sinonimo di esplicito. Anche una manifestazione implicita di volontà può infatti reputarsi idonea a soddisfare tale requisito, ma non può essere comunque tacita, perché l'inerzia del soggetto non può essere interpretata come consenso. Quest'ipotesi si verificherebbe ad esempio utilizzando form precompilati o anche l'abusata prassi delle caselle già spuntate. Ben diverso è il caso della richiesta di spuntarle, essendo già predisposte, in modo tale che evidenzino la volizione del soggetto cui pertengono i dati. Lo stesso con riguardo alla richiesta di inserimento di indirizzo e-mail in apposito campo della cui ben individuata finalità si dia contezza. Casi speciali (art. 9 GDPR) vengono configurati dal trattamento dei dati particolari o comunque confluenti in processi decisionali automatizzati, equiparabili sotto il profilo del consenso che deve essere esplicito. Tra questi ultimi rientra a pieno titolo la profilazione. Per l'attività dei media non vengono prescritte forme particolari, a prescindere dal tipo di dato oggetto di trattamento. Profilazione (lett. e) s'intende qualsiasi forma di trattamento automatizzato di dati personali utilizzati per valutare determinati aspetti personali, in particolare per analizzare o prevedere il rendimento professionale, la situazione economica, la salute, le preferenze, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti. Ben diversamente deve intendersi la c.d. profilazione criminale, o definizione del profilo criminale (criminal profiling, o criminal investigative analysis), che si risolve in uno strumento investigativo finalizzato ad individuare una persona/soggetto criminale totalmente o parzialmente sconosciuta e che per sua natura si presta e può essere finalizzata talvolta alla diffusione di dati parziali, non ancora attribuibili ad un determinato individuo, per fini investigativi di ricerca, generalmente repressivi. Archivio (lett. f) s'intende un qualsiasi insieme strutturato di tali dati. Autorità competente (lett. g, 1) è qualsiasi autorità pubblica nazionale, di Stato U.E. o terzo, competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, inclusa la prevenzione di minacce alla sicurezza pubblica; (lett. g, 2) oltre a qualsiasi altro organismo o entità incaricato dagli ordinamenti interni di esercitare l'autorità pubblica e pubblici poteri agli stessi fini. Violazione dei dati personali (lett. m) viene intesa quella concernente la sicurezza che comporti accidentalmente o in modo illecito la loro distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a quelli trasmessi, conservati o comunque trattati. Dati genetici (lett. n) sono quelli relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscano informazioni univoche sulla sua fisiologia o salute e che risultano in particolare dall'analisi di un campione biologico. Dati biometrici (lett. o) sono quelli ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali che consentano o confermino l'identificazione univoca (es. immagine facciale o dati dattiloscopici). Dati relativi alla salute (lett. p) sia fisica che mentale, compresa la prestazione di servizi di assistenza sanitaria che la rivelino. File di log (lett. q) è inteso il registro degli accessi e delle operazioni. I principi da seguire prevedono (art. 3): trattamento lecito e corretto; raccolta per finalità determinate, espresse e legittime e con modalità compatibili con tali finalità; adeguatezza, pertinenza e non eccedenza rispetto alle finalità; esattezza e, se necessario, loro aggiornamento (adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti); conservazione con modalità che consentano l'identificazione degli interessati per il tempo necessario al conseguimento delle finalità proprie; esame periodico per verificarne la persistente necessità di conservazione, considerandone la cancellazione o anonimizzazione decorso il termine; un'adeguata sicurezza e protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali, attraverso misure tecniche e organizzative adeguate. Di particolare interesse risulta la distinzione in categorie degli interessati oltre che dei dati (art. 4) considerando che esplica effetti sulla relativa conservazione e verifica della qualità. I soggetti vengono distinti in base alle diverse categorie d'appartenenza (secondo legge): persone sottoposte a indagine; imputati; persone sottoposte a indagine o imputate in procedimento connesso o collegato; persone condannate con sentenza definitiva; persone offese dal reato; parti civili; persone informate sui fatti; testimoni. Quanto ai dati si distingue tra quelli fondati su fatti e quelli fondati su valutazioni. Il trattamento automatizzato dei dati reso talvolta indispensabile dalla mole delle informazioni esistenti, acquisibili o da processare (es. nella profilazione antiriciclaggio, esige l'intervento umano nel

momento decisionale, laddove conseguenze sfavorevoli possano discenderne (art. 23 GDPR). A fattor comune viene previsto che le autorità competenti adottino misure adeguate a garantire che i dati personali inesatti, incompleti o non aggiornati non siano trasmessi (comunicati) o resi disponibili (es. in banche dati), altresì verificandone la qualità prima che giungano ad altre autorità (nazionali o estere), corredando la comunicazione di informazioni tali da consentire anche a queste ultime di valutarne il grado di esattezza, completezza, aggiornamento e affidabilità. Quando risulti che i dati siano stati trasmessi illecitamente o siano inesatti, il destinatario ne deve essere tempestivamente informato, rettificandoli o cancellandoli. Il diritto all'oblio (art. 17 GDPR) prevede deroghe quando il trattamento abbia un fondamento giuridico diverso dal consenso che invece, come detto, presuppone un'informativa che indichi tra l'altro la durata della conservazione dei dati. Deroghe ricorrono nell'antiriciclaggio e nella tenuta delle banche dati delle FFPP. In generale si prevede che l'interessato che ne abbia il diritto possa ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardino e che detto titolare abbia l'obbligo di cancellarli senza ingiustificato ritardo. In ogni caso l'interessato può opporsi al trattamento ove non sussista alcun motivo legittimo prevalente per procedervi o se i dati personali siano stati trattati illecitamente. La valenza transnazionale dell'antiriciclaggio e del contrasto al finanziamento del terrorismo, per l'U.E. desumibile dalla IV e V Direttiva, deve ritenersi valore preminente e prevalente, garantendo un'interpretazione, che non rechi vulnus al quadro delineatosi a seguito di una ultraventennale evoluzione. I richiamati diritti della persona interessata, in ogni caso, non possono assurgere a valore preminente rispetto alla comunicazione di dati personale all'A.G. per il procedimento e il processo penale o per l'esecuzione della pena; lo stesso può dirsi per la comunicazione di dati all'autorità amministrativa per le esigenze del procedimento di applicazione di misure di sicurezza o di prevenzione o sanzionatorio.

Phishing e trattamento illecito di dati personali si ha da parte di chi, soprattutto utilizzando le possibilità offerte dalla rete ed in genere attraverso l'invio di una e-mail che simula il contatto con una banca o nell'ambito del commercio elettronico (B2C), invita a comunicare dati personali, numero di carta di credito, codici per l'home banking, con motivazioni plausibili e suggestive, malgrado l'utenza venga sempre ammonita a tale riguardo da tutti gli istituti di credito. Può configurarsi, in questo caso, la fattispecie di trattamento illecito di dati personali, sotto il profilo di un'**acquisizione fraudolenta di dati personali** (art. 167 – ter) quando ciò avvenga su larga scala, sanzionando quindi chi acquisisca con tali modalità un archivio automatizzato (o una parte sostanziale), contenente dati personali oggetto di trattamento su larga scala al fine di trarne profitto o di arrecare danno ad altri. Il GDPR (art. 84) rinvia l'aspetto sanzionatorio ai singoli Stati membri, imponendo al legislatore nazionale l'introduzione d'una previsione del danno come elemento caratterizzante tale reato, oltre allo scopo di profitto. Rileva quindi, per la configurazione della fattispecie, il profitto dell'autore ma anche il danno patito dalla vittima, inclusi quello d'immagine e di reputazione, che implica (quest'ultimo) il c.d. *revenge porn*. Viene inoltre previsto il coordinamento tra il PM e l'Autorità di controllo, senza ritardo. Per completezza, le fattispecie di reato in materia contemplano: trattamento illecito di dati (art. 167); comunicazione e diffusione illecita di dati personali (art. 167 bis); acquisizione fraudolenta di dati personali (art. 167 ter); interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante (art. 168); inosservanza di provvedimenti del Garante (art. 170); violazioni in materia di controlli a distanza dei lavoratori. L'art. 168 citato punisce chiunque, in un procedimento o nel corso di accertamenti dinanzi all'Autorità di Controllo, dichiari o attesti falsamente notizie o circostanze o produca atti o documenti falsi.
Inoltre sanziona penalmente (c. 2) chi cagioni intenzionalmente un'interruzione o turbi la regolarità di un procedimento dinanzi al Garante o degli accertamenti da questi svolti.

L'ipotesi di truffa (art. 640 cp, c. 1), può essere valutata per … chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno …

La truffa aggravata (art. 640 cp, c. 2) ricorre quando il fatto risulti commesso ingenerando nella persona offesa il timore di un pericolo o l'erroneo convincimento di dover eseguire l'ordine di un'autorità.

GIURISPRUDENZA

USO DELLA FORZA - l'uso della forza limitato a quanto strettamente necessario è legittimato dalla necessità di adempimento del servizio di polizia e dall'illecito comportamento del trasgressore, nel caso in cui per la sua identificazione occorra procedere all'accompagnamento in ufficio (Cass. civ. Sez. III, 3.9.2007, n. 18531). Una volta identificato, procedere alla notifica del verbale di elezione di domicilio e nomina del difensore di fiducia (in mancanza del quale ne sarà assegnato uno d'ufficio), ed alla comunicazione prevista dall'art. 347 c.p.p. per deferirlo all'A.G. competente. Nel caso il soggetto rifiuti di declinare le proprie generalità e successivamente, dietro insistenze, non esclusa la prospettiva di un accompagnamento coattivo, ottemperi tardivamente, è necessario procedere comunque alla redazione del verbale di elezione di domicilio e nomina del difensore di fiducia (in difetto d'ufficio). È irrilevante che le notizie circa l'identità del soggetto siano facilmente accessibili dall'agente operante.

LIMITE

La Convenzione Europea dei Diritti dell'Uomo (CEDU, in vigore dal 1953), riflettendo il contenuto della Dichiarazione Universale dei Diritti dell'Uomo (approvata dall'Assemblea Generale delle Nazioni Unite il 10 dicembre 1948 a Parigi), prevede quattro sostanziali garanzie: diritto alla vita (art. 2), proibizione della tortura (art. 3), proibizione della schiavitù e del lavoro forzato (art. 4), diritto alla libertà e alla sicurezza (art. 5). Era da poco finita la Seconda Guerra Mondiale e i due principali strumenti tutelari di diritto internazionale non erano stati pensati per le persone private della libertà personale a seguito di crimini (detenuti) o in fase d'indagine per gravi comportamenti costituenti reato, avendo semmai d'occhio le recenti aberrazioni dei campi di sterminio e di lavoro, oltre che le molte situazioni di compromissione dei diritti umani operate dai regimi di vario colore, alcuni usciti sconfitti dal conflitto, altri vittoriosi e ancora ben vitali. Cionondimeno sin da subito buona parte dei ricorsi presentati alla Commissione Europea dei Diritti Umani concerneva persone in condizioni di detenzione a vario titolo. Altri e più specifici strumenti si sono nel frattempo aggiunti per la protezione di coloro che vengono privati, a vario titolo, della libertà personale: la *Convenzione Contro la Tortura ed Altre Pene o Trattamenti Crudeli, Disumani o Degradanti* (1984), la *Convenzione Europea per la Prevenzione della Tortura e delle Pene o Trattamenti Inumani o Degradanti* (1987) e *le Regole Penitenziarie Europee* (2006). Il ricorso individuale previsto dalla Convenzione viene consentito anche a fronte di decisioni sfavorevoli da parte del Giudice nazionale e qui si vogliono evidenziare regole comportamentali che tengano conto delle pronunce della Corte di Strasburgo (CEDU).

Una violazione procedurale e sostanziale dell'art. 3 della CEDU (*nessuno può essere sottoposto a tortura né a pene o trattamenti inumani o degradanti*) è stata ritenuta sussistere a carico del nostro Paese affermando (ovviamente) il divieto di comportamenti lesivi della dignità umana da parte dell'autorità di polizia e sancendo soprattutto l'obbligo di indagini approfondite sulle presunte violazioni da parte della stessa, in particolare durante la detenzione o comunque nelle fasi procedurali che vedano la privazione della libertà personale. I fatti giudicati avevano peraltro formato oggetto di esaustiva verbalizzazione e gli operanti avrebbero fatto uso della forza solo a fronte di un comportamento violento dello stesso ricorrente, in particolare questi avrebbe gettato fuori da una finestra una loro dotazione poi aggredendoli. Il punto debole della procedura nazionale andrebbe ricercato, secondo la CEDU nel caso di specie, nella laconicità del decreto di archiviazione del procedimento conseguente alla denuncia presentata nei confronti degli agenti da parte della sedicente vittima. Tale provvedimento non avrebbe tenuto conto della necessità di una più ampia motivazione dell'atto decisorio e dell'insufficienza delle presupposte attività d'indagine (del P.M. e della P.G. delegata) che nello specifico non avrebbero eseguito neppure un interrogatorio dei diversi soggetti coinvolti, pur risultando concordi le loro dichiarazioni circa il fatto che le lesioni refertate alla vittima fossero conseguenza della coazione fisica posta in essere dalla P.G. presso il proprio comando.

La pronuncia favorevole al ricorrente è avvenuta nel solco di un consolidato orientamento circa la presunta violazione della Convenzione (art. 3 cit.) da parte della forza pubblica, quando i fatti accadano in condizioni di menomata libertà della vittima, e al necessario onere probatorio (sentenza Bouyid – Belgio - ricorso 23380/2009) da soddisfare per liberare lo Stato degli inquirenti/inquisiti da responsabilità. Qualora i fatti di violenza avvengano durante la detenzione, a qualsiasi titolo operata, devono ritenersi di esclusiva conoscenza (o conoscibilità?) della P.G. registrandosi quindi, a tale riguardo, la necessità di una vera e propria inversione dell'onere della prova. Quanto precede pur se le accuse di maltrattamenti subiti ad opera dei poliziotti (in veste stavolta di imputati) necessitino di elementi probatori forti nei loro confronti, tali da giustificarne una condanna al di là di ogni ragionevole dubbio.

In ogni caso se una denuncia di fatti della specie viene presentata alle autorità requirenti nazionali, queste devono svolgere con zelo le necessarie indagini sugli accadimenti avvenuti durante la custodia, durante il quale l'Autorità è tenuta, a garantire l'incolumità delle persone che vi soggiacciono.

La Cedu ha ritenuto che anche solo uno schiaffo, senza conseguenze fisiche, inferto al volto da parte della polizia nei confronti di un individuo che si trovi completamente soggetto al suo controllo, costituisca un grave attacco alla dignità umana, integrando un ***trattamento degradante***, poiché il viso rappresenta la parte del corpo che esprime l'individualità della persona, che manifesta la sua identità sociale e che costituisce il centro dei suoi sensi (vista, parola e udito) utilizzati anche per la comunicazione col prossimo (28 settembre 2015). Il ricorso all'uso della forza che non trovi giustificazione dalla stessa condotta dell'individuo, ne svilisce la dignità e rappresenta in via di principio un caso di ***police brutality*** (violazione dell'art. 3 Cedu).

La vittima può sentirsi umiliata anche da uno schiaffo, *per quanto isolato, non premeditato e privo di effetti gravi o duraturi sul corpo,* proprio perchè viene percepito come un'umiliazione, perchè sottolinea la relazione di *superiorità-inferiorità* che per definizione caratterizza il rapporto tra l'autorità e l'individuo in custodia. Il fatto che la vittima abbia la consapevolezza che l'atto violento integri un illecito *deontologico e professionale* da parte della polizia potrebbe suscitare inoltre un senso di arbitrarietà, di ingiustizia e d'impotenza, senza contare che, proprio per la sua risibile efficacia in termini coercitivi, non può trovare una giustificazione nella necessità di prevalere durante l'illecito comportamento tenuto dal trasgressore.

Frode informatica

Il phishing integra frode informatica (art. 640-ter cp), presupponendo *… un'alterazione del funzionamento di un sistema informatico o un intervento abusivo sul sistema stesso o su dati o informazioni o programmi ivi contenuti o ad esso pertinenti, così da determinare un ingiusto profitto per il soggetto attivo e un danno per il soggetto passivo* … (Trib. Padova n. 75/2013).

L'accesso abusivo ad un sistema informatico o telematico (art. 615 ter cp, c. 1) può essere rubricato nei confronti del phisher ricorrendone gli estremi (Tribunale Milano GIP n. 13/2013).

Il phishing può integrare il delitto di sostituzione di persona (art. 494 cp) attraverso la falsa dichiarazione o attestazione sull'identità o su qualità personali proprie o di altri. Pur mancando la materiale sostituzione della persona, il furto d'identità risulta infatti prodromico all'utilizzo degli estremi identificativi di un soggetto, (credenziali) per eseguire l'accesso a sistemi informatici, eseguendo pagamenti o apprensioni di denaro e disponibilità indebiti (S.C. Pen. n. 46674/2007).