Npl, attesi 83 miliardi di euro di transazioni per fine 2018
9 ottobre 2018

Il grande abbaglio: State of Florida vs Chico Forti
8 ottobre 2018

Paolo Corradino della BCE: “Il lavoro di supervisione è stato utile, ma servono ulteriori sforzi”
8 ottobre 2018

Euler Hermes lancia sul mercato Identity One, la prima polizza contro il furto d’identità commerciale
8 ottobre 2018

Gestione del credito

9 ottobre 2018

L’insostenibile leggerezza della Data Retention

a cura di Paolo Calabretta
tastiera all'esperto

Uno dei temi più delicati che, in vari settori professionali, impegna gli operatori è quello della *data retention* dei dati personali.

L’argomento della *data retention* dei dati personali è stato recentemente trattato nella relazione tenuta dall’**Avv. Marco Recchi** nel corso del Seminario: **Privacy Day – La guida operativa per le società di informazione e gestione del credito**, organizzato da *StopSecret Magazine* e tenutosi a Roma in data **20 Settembre 2018**.

D’altronde, come pure esposto nel corso della suindicata relazione, **l’art. 13, 2° comma del GDPR**, dispone che già nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all’interessato – tra le varie informazioni necessarie per garantire un trattamento corretto e trasparente – anche **il periodo di conservazione dei dati personali** oppure, se non è possibile, i criteri utilizzati per determinare tale periodo.

Con il presente scritto, si vuole evidenziare come – sia prima, che dopo – l’entrata in vigore del GDPR e, ora, del Dlgs. 10 Agosto 2018, n. 101, si siano stratificate varie discipline settoriali contenute:
-sia in codici di deontologia e di buona condotta pubblicati in Gazzetta Ufficiale;
-che in singoli testi legislativi;
-che in linee guida emanate da organismi di rappresentanza istituzionale di categoria professionale e, segnatamente, dell’avvocatura italiana.

Si metteranno, ora, a confronto, **tre regolamentazioni in settori diversi**, ma sempre di interesse per l’operatore di diritto, per poi trarne, alla fine, le relative conclusioni e suggerire soluzioni operative.

I°

In materia di investigazioni private, il tema in oggetto è stato già da diversi anni così cogente, che con Decreto Min. Giustizia del 02-12-2008, in G.U., parte I, 24-12-2008 n. 300, è stato pubblicato il *Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o per far valere o difendere un diritto in sede giudiziaria, in particolare da liberi professionisti o da soggetti che esercitano un’attività di investigazione privata autorizzata in conformità alla legge, ai sensi dell’articolo 12, comma 2 del decreto legislativo 30 giugno 2003, n. 196.*

E ciò *Vista la documentazione trasmessa dal Garante per la protezione dei dati personali e, in particolare, la deliberazione di tale Autorità n. 60 del 6 novembre 2008 che ha verificato la conformità alle leggi e ai regolamenti del codice di deontologia e di buona condotta per i dati trattati per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria, sottoscritto dall’**AIGA** – Associazione italiana giovani avvocati, dal **CNF** – Consiglio nazionale forense, dall’**OUA** – Organismo unitario dell’avvocatura italiana, dall’**UAE** – Unione avvocati europei, dall’**UCPI** – Unione camere penali italiane, dall’**UNCC** – Unione nazionale camere civili, dall’**AIPROS** – Associazione italiana professionisti della sicurezza, dalla **FEDERPOL** – Federazione italiani istituti investigazioni-informazioni-sicurezza, e ha disposto la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana (Gazzetta Ufficiale n. 275 del 24 novembre 2008);*

Ebbene, all’art. 10 di tale Codice Deontologico (costituente allegato A.6 del Dlgs. 196/2003) prevede che:

Art. 10. Conservazione e cancellazione dei dati

1.Nel rispetto dell´art. 11, comma 1, lett. e) del Codice i dati personali trattati dall´investigatore privato possono essere conservati per un periodo non superiore a quello strettamente necessario per eseguire l´incarico ricevuto. A tal fine deve essere verificata costantemente, anche mediante controlli periodici, la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto alle finalità perseguite e all´incarico conferito.

2.Una volta conclusa la specifica attività investigativa, il trattamento deve cessare in ogni sua forma, fatta eccezione per l´immediata comunicazione al difensore o al soggetto che ha conferito l´incarico, i quali possono consentire, anche in sede di mandato, l´eventuale conservazione temporanea di materiale strettamente personale dei soggetti che hanno curato l´attività svolta, a i soli fini dell´eventuale dimostrazione della liceità e correttezza del proprio operato. Se è stato contestato il trattamento il difensore o il soggetto che ha conferito l´incarico possono anche fornire all´investigatore il materiale necessario per dimostrare la liceità e correttezza del proprio operato, per il tempo a ciò strettamente necessario.

3.La sola pendenza del procedimento al quale l´investigazione è collegata, ovvero il passaggio ad altre fasi di giudizio in attesa della formazione del giudicato, non costituiscono, di per se stessi, una giustificazione valida per la conservazione dei dati da parte dell´investigatore privato.

In merito a tale regolamentazione, interessante è il commento dell’Avv. **Roberto Gobbi** a suo tempo pubblicato su questa rivista (clicca qui per leggere l’articolo).

II°
Una ulteriore regolamentazione in tema di *data retention* – pure essa anteriore all’entrata in vigore del GDPR e, ora, del Dlgs. 10 Agosto 2018, n. 101 (ma, stavolta, introdotta con apposita legge) – si rinviene in materia di **Organismi di composizione della crisi** di cui alla Legge 27/01/2012 n. 3, rubricata Disposizioni in materia di usura e di estorsione, nonche’ di composizione delle crisi da **sovraindebitamento**, il cui art. 15, 11° comma, così dispone:

“I dati personali acquisiti a norma del presente articolo possono essere trattati e conservati per i soli fini e tempi della procedura e devono essere distrutti contestualmente alla sua conclusione o cessazione. Dell’avvenuta distruzione e’ data comunicazione al titolare dei suddetti dati, tramite lettera raccomandata con avviso di ricevimento o tramite posta elettronica certificata, non oltre quindici giorni dalla distruzione medesima”.

III°
Ora – posto che le prima e la seconda delle fattispecie suesposte sono antecedenti all’entrata in vigore del GDPR e, ora, del Dlgs. 10 Agosto 2018, n. 101 – veniamo ad esaminare la normativa introdotta dal Regolamento Europeo in materia di diritto alla cancellazione dei dati.

Ebbene, l’Art. 17 del **Regolamento generale sulla Protezione dei dati (Regolamento (UE)** 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016) così come modificato dal provvedimento di “*Rettifica del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 …*”, dispone quanto segue:

Articolo 17
Diritto alla cancellazione («diritto all’oblio»)

> L’interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l’obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
> a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
> b) l’interessato revoca il consenso su cui si basa il trattamento conformemente all’articolo 6, paragrafo 1, lettera a), o all’articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
> c) l’interessato si oppone al trattamento ai sensi dell’articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell’articolo 21, paragrafo 2;
> d) i dati personali sono stati trattati illecitamente;
> e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell’Unione o dello Stato membro cui è soggetto il titolare del trattamento;
> f) i dati personali sono stati raccolti relativamente all’offerta di servizi della società dell’informazione di cui all’articolo 8, paragrafo 1.
> Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell’interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
> I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
> a) per l’esercizio del diritto alla libertà di espressione e di informazione;
> b) per l’adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell’Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l’esecuzione di un compito svolto nel pubblico interesse oppure nell’esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell’articolo 9, paragrafo 2, lettere h) e i), e dell’articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all’ articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) per l’accertamento, l’esercizio o la difesa di un diritto in sede giudiziaria.

Veniamo, quindi, ad un settore, quello forense, per il quale – a seguito dell’entrata in vigore del GDPR – l’organo rappresentativo dell’Avvocatura, e cioè il Consiglio Nazionale Forense, ha emanato apposite linee guida.

La Commissione del CNF in materia di privacy, nelle sue linee guida, denominate: *Il GDPR e l’avvocato* (e, quindi, all’indomani dell’entrata in vigore del GDPR), così si è espressa:

Conservazione dei dati
L’avvocato titolare del trattamento deve definire una politica di durata e di conservazione dei dati nel suo ufficio. I dati personali possono essere conservati solo per il tempo necessario per il completamento dell’obiettivo perseguito durante la loro raccolta.

In generale, i dati dei clienti possono essere tenuti per la durata del mandato professionale tra l’avvocato e il suo cliente. Possono ovviamente essere conservati anche dopo la cessazione del rapporto professionale, al fine di tutelare i diritti dell’avvocato nei confronti del cliente, sia quanto al diritto a conseguire i compensi, sia per resistere ad eventuali azioni di responsabilità: per tale ragione, si ritiene che la conservazione dei dati possa prolungarsi per tutto il tempo di prescrizione ordinaria, prima della loro cancellazione definitiva.

È inoltre importante ricordare che i dati acquisiti in sede di identificazione e adeguata verificata ai sensi del decreto legislativo n. 231 del 2007 in materia di antiriciclaggio devono essere conservati per un periodo di 10 anni dalla cessazione del rapporto continuativo, della prestazione professionale o dall’esecuzione dell’operazione occasionale (art. 31, comma 3, d. lgs. 231 del 2007) >>.

Clicca qui per consultare il testo

Peraltro, a tutte le disposizioni normative come sopra richiamate dal **CNF**, andrebbe aggiunta (e non per ultimo) la **normativa fiscale**, dalla quale pure scaturisce l’esigenza di rispettare il più ampio termine di conservazione ivi indicato.

Conclusioni
Una volta passata in rassegna la regolamentazione relativa tali specifici settori, possono svolgersi le seguenti considerazioni con riferimento ai suindicati settori, come sopra regolamentati in data antecedente al GDPR.

In materia di investigazioni private
Con riferimento all’attività di investigazioni private, a mio avviso, potrebbe trovare applicazione il suindicato comma 3° lettera e) dell’art. 17 del Regolamento, sicchè può ritenersi che il titolare del trattamento non abbia l’obbligo di cancellare i dati personali, essendo, di contro, tale conservazione necessaria per l’accertamento, l’esercizio o la difesa di un diritto in sede giudiziaria.

Valgono, all’uopo – *mutatis mutandis* – le medesime considerazioni sopra espresse in ordine alle esigenze di *data retention* per l’attività forense.

Epperò, all’art. 20 del Decreto Legislativo n. 101/2018 (in G. U. n. 205 del 4-9-2018), leggesi quanto segue (si attenzionino le parti evidenziate):

Codici di deontologia e di buona condotta vigenti alla data di entrata in vigore del presente decreto

Le disposizioni del codice di deontologia e di buona condotta di cui agli allegati A.5 e A.7 del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, continuano a produrre effetti, sino alla definizione della procedura di approvazione cui alla lettera b), a condizione che si verifichino congiuntamente le seguenti condizioni:
a) entro sei mesi dalla data di entrata in vigore del presente decreto le associazioni e gli altri organismi rappresentanti le categorie interessate sottopongano all’approvazione del Garante per

la protezione dei dati personali, a norma dell’articolo 40 del Regolamento (UE) 2016/679, i codici di condotta elaborati a norma del paragrafo 2 del predetto articolo;

b) la procedura di approvazione si concluda entro sei mesi dalla sottoposizione del codice di condotta all’esame del Garante per la protezione dei dati personali.
Il mancato rispetto di uno dei termini di cui al comma 1, lettere a) e b) comporta la cessazione di efficacia delle disposizioni del codice di deontologia di cui al primo periodo a

decorrere dalla scadenza del termine violato.

*Le disposizioni contenute nei codici riportati negli allegati A.1, A.2, A.3, A.4 e **A.6** del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, **continuano a produrre effetti fino alla pubblicazione delle disposizioni ai sensi del comma 4.***
Entro novanta giorni dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali verifica la conformita’ al Regolamento (UE) 2016/679 delle disposizioni di cui al comma 3. Le disposizioni ritenute compatibili, ridenominate regole deontologiche, sono pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, sono successivamente riportate nell’allegato A del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003.
Il Garante per la protezione dei dati personali promuove la revisione delle disposizioni dei codici di cui al comma 3 con le modalita’ di cui all’articolo 2-quater del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003.

Ne deriva come appaia opportuno – sussistendo per i soggetti che svolgono attività di investigazione privata le medesime esigenze di conservazione dei dati come sopra indicate dalla Commissione del CNF in materia di *privacy* – che venga sollecitata la revisione del Codice Deontologico, nei termini e con le modalità come sopra previste dal summenzionato art. 20 Dlgs. n. 101/2018.

E ciò onde recepire nelle relative regole deontologiche da (ri)elaborare in materia di investigazioni private – *expressis verbis* – le disposizioni del suindicato comma 3° lettera e) dell’art. 17 del Regolamento generale sulla protezione dei dati (Regolamento (UE) 2016/679.

D’altronde, potrà invocarsi quale rilevante termine di comparazione il richiamo ai medesimi principi come sopra elaborati dal CNF (ed anche in questo caso, aggiungendovi le ulteriori considerazioni che impongono il rispetto del termine di conservazione imposto dalla normativa fiscale ed, ancora, i diversi termini imposti dal rispetto del T.U. LEGGI DI PUBBLICA SICUREZZA T.U.L.P.S.): e ciò secondo il noto brocardo: *Ubi eadem legis ratio, ibi eadem legis dispositio* e cioè Dov’è una stessa ragione di legge, ivi deve aver vigore la medesima norma.

Organismi di composizione della crisi

Dall’esame del GDPR, può ritenersi come anche per gli Organismi di composizione della crisi soccorra il suindicato comma 3° lettera e) dell’art. 17 del REGOLAMENTO, sicchè può ritenersi che il titolare del trattamento non abbia l’obbligo di cancellare i dati personali, essendo, di contro, tale conservazione necessaria per l’accertamento, l’esercizio o la difesa di un diritto in sede giudiziaria.

Altresì, ritengo trovi pure applicazione il comma 3° lettera b) del medesimo art. 17.

Sicchè – a mio sommesso avviso – l’obbligo di cancellazione dei dati di cui all’art. 15, 11° comma Legge 27/01/2012 n. 3, incombente sugli Organismi di composizione della crisi – dovrebbe considerarsi tacitamente abrogato, applicando i principi di cui alla seguente massima:

Ai sensi dell’art. 15 disp. prel. c.c., l’abrogazione tacita di una legge ricorre quando sussiste incompatibilità fra le nuove disposizioni e quelle precedenti, ovvero quando la nuova legge disciplina la materia già regolata da quella anteriore; in particolare, la suddetta incompatibilità si verifica solo quando fra le leggi considerate vi sia una contraddizione tale da renderne impossibile la contemporanea applicazione, cosicché dall’applicazione ed osservanza della nuova legge derivi necessariamente la disapplicazione o l’inosservanza dell’altra.

Cassazione civile, sez. I, 21/02/2001, n. 2502.

Invero, l’art. 17 del GDPR, come risulta dalla sua rubrica, regolamenta in maniera sistematica il Diritto alla cancellazione («diritto all’oblio»).

Senza dire che – in fattispecie analoghe – altra legge speciale e cioè l’art. 31 bis 3° comma Legge Fallimentare dispone, invece, che: *III. In pendenza della procedura e per il periodo di due anni dalla chiusura della stessa, il curatore e’ tenuto a conservare i messaggi di posta elettronica certificata inviati e ricevuti.*

Sicchè, a ben vedere – già prima dell’entrata in vigore del GDPR – vi erano elementi per invocare, quanto meno, un’illegittimità costituzionale della norma, per disparità di trattamento per casi analoghi e ciò in violazione del principio costituzionale di uguaglianza.

Gestione del credito

in evidenza

Roadshow Innovation HR arriva a Roma, il 10 ottobre

I più letti

Il grande abbaglio: State of Florida vs Chico Forti

Npl, attesi 83 miliardi di euro di transazioni per fine 2018

Salvini: massimo sostegno alla vigilanza privata

NPL, dalle banche ai servicer. È la “Rivoluzione industriale” del credito?

Il biotecnologo forense

L’antifrode assicurativa dell’Investigatore Privato

Differenze fra le attività d’informazioni commerciali e d’investigazione

Privacy, pubblicato il decreto attuativo del GDPR

Paolo Corradino della BCE: “Il lavoro di supervisione è stato utile, ma servono ulteriori sforzi”

Npl, il report di Kpmg sulle banche italiane

Verso il riconoscimento di Polizia Giudiziaria per le Guardie Particolari Giurate

Euler Hermes lancia sul mercato Identity One, la prima polizza contro il furto d’identità commerciale

Il Risk Manager: chi è, cosa fa, le competenze, l’evoluzione

Minacciare azioni legali per crediti inesistenti è estorsione

Roadshow Innovation HR arriva a Roma, il 10 ottobre

Ti potrebbero interessare...

Intercettazioni domiciliari: legittime solo per attività criminose

Investigare e fornire informazioni cosa sono?

Falsa malattia, le aziende si affidano agli investigatori privati

NPL: ACCORDO TRA INTESA SANPAOLO E INTRUM

Banche: servono soluzioni per gli Utp

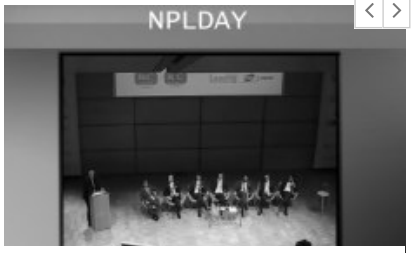
TV

Gli ultimi video

Fiera del Credito 2018 - Focus a cura di ANC - Ass. Naz.le Commercialisti

Fiera del Credito 2018 - Focus a cura di Creden S.p.A.

Fiera del Credito 2018 - Focus a cura di Mauro Cammarata



Fiera del Credito 2018 - NPL Day

StopSecret EVENTI

Investigation & Forensic Award 2018

Credit Management & Collection Awards 2019

ISCRIVITI ALLA NEWLETTER

MENU PRINCIPALE

StopSecret
MAGAZINE • TV • EVENTI

Informativa privacy
Redazione
Contatti

Direttore Editoriale: Cosimo Cordaro
Direttore Responsabile: Katja Casagranda
Proprietario: Stop Secret S.r.l.
Iscritto nel Registro della Stampa del Tribunale di Milano
al nr. 309 del 18/09/2014

web by www.altrarete.it

SITI WEB CORRELATI

FIERA DEL CREDITO
www.fieradelcredito.it

CREDIT MANAGEMENT & COLLECTION AWARDS 2019
creditmanagementcollectionawards

INVESTIGATION & FORENSIC AWARDS 2018
investigationforensicawards2018

Home
Informazioni commerciali
Gestione del credito
Investigazioni
Vigilanza e sicurezza
Tutto intorno
Stopsecret TV
Eventi
Autori
Contatti