Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

AGOSTO – SETTEMBRE 2015

Diritto d'autore sulle foto pubblicate sui social network

Una recente sentenza del Tribunale di Roma precisa che la pubblicazione di foto sui social network, nella pagina di chi le ha scattate "non comporta la cessione integrale dei diritti fotografici".

Dal punto di vista normativo, nulla di nuovo, in quanto è risaputo che ciò che si scarica da Internet, che siano testi o immagini, non sempre è liberamente utilizzabile. La sentenza in esame, nell'applicare la normativa vigente, altro non fa che confermare la necessità di verificare se l'uso del materiale scaricato dal web è libero oppure occorre apposita autorizzazione/liberatoria di chi ne detiene i diritti d'autore.

Il caso risulta interessante in quanto la pubblicazione delle foto è stata fatta su un social network, e la sentenza risponde al quesito che ci siamo posti di frequente "Quando pubblico le foto sul mio profilo di un qualsiasi social network, io autore delle foto, cedo inconsapevolmente tutti i diritti al social network stesso, oppure rimango titolare dei diritti d'autore?". Il Tribunale di Roma ha così sentenziato: "la pubblicazione di foto sui social network, nella pagina di chi le ha scattate, non comporta la cessione integrale dei diritti fotografici".

Inoltre, la sentenza riconosce il danno provocato all'autore delle foto, in seguito alla loro pubblicazione da parte di un quotidiano, senza aver richiesto preventiva autorizzazione/liberatoria dell'autore. Il solo fatto che le foto fossero pubblicate sul social network non le rendeva di pubblico utilizzo.

Detto ciò, il Tribunale ha esaminato le condizioni di licenza del social network coinvolto, ed ha stabilito che "la possibilità di utilizzo delle informazioni pubblicate con impostazione 'Pubblica' sul social network non costituisce licenza generalizzata di utilizzo e di sfruttamento dei contenuti coperti da diritti di proprietà intellettuale in favore di qualunque terzo che accede alla pagina". Al contrario la libertà di utilizzo

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

"riguarda esclusivamente le informazioni e non i contenuti coperti da diritti di proprietà intellettuale".

In conclusione, anche se "postate" in modalità pubblica, le immagini rimangono di proprietà dell'autore, fino a prova contraria, e l'uso da parte di terzi non è legittimo senza specifica autorizzazione dell'autore.

Riferimenti: Sentenza del Tribunale di Roma n. 12076/15 del 1° giugno 2015

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

La "Legge Europea 2014" aggiorna il Codice delle comunicazioni elettroniche e il Testo unico dei servizi media audiovisivi e radiofonici

La Legge Europea 2014 di recepimento della normativa comunitaria, volta a garantire l'adeguamento dell'ordinamento nazionale a quello europeo, ha apportato alcune modifiche al vigente Codice delle comunicazioni elettroniche (Dlgs 259/2003) e al Testo unico dei servizi di media audiovisivi e radiofonici (art. 24, Dlgs 177/2005) in materia di:
- impianti ed esercizio di stazioni radioelettriche a bordo di navi;
- servizi di radiodiffusione sonora in onde medie a modulazione di ampiezza;
- costi amministrativi a carico dei fornitori di servizi di comunicazioni elettroniche.

Le modifiche introdotte dalla Legge europea 2014 entrano in vigore il 18 agosto 2015.

Riferimenti: Legge 29 luglio 2015, n. 115 "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2014" (G.U. n. 178 del 3 agosto 2015).

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Il processo tributario diventa telematico

Il Ministero dell'economia e delle finanze rende note le specifiche tecniche che consentono l'attuazione del D.M. 23 dicembre 2013, n. 163 (emanato per attuare la norma prevista dal D.L. n. 98/2011, art. 39) che contiene regole operative per l'applicazione degli strumenti informatici alle Commissioni tributarie. Le prime ad essere telematizzate saranno le Commissioni tributarie provinciali e regionali di Toscana ed Umbria, per estendere, dopo una fase sperimentale iniziale, la telematizzazione alle Commissioni provinciali e regionali sul territorio nazionale.

Fase transitoria
Le presenti disposizioni si applicano agli atti processuali relativi ai ricorsi notificati presso le Commissioni tributarie provinciali e regionali dell'Umbria e della Toscana, a partire dal 1° dicembre 2015. Rimaniamo in attesa di apposito decreto legislativo di riforma "complessiva" del processo tributario.

Riferimenti: Decreto Ministero dell'economia e delle finanze 4 agosto 2015 (GU Serie Generale n.184 del 10-8-2015)

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Riforma della pubblica amministrazione: Carta della cittadinanza digitale

L'articolo 1 della legge delega al Governo in materia di riorganizzazione delle amministrazioni pubbliche è la Carta della cittadinanza digitale: viene così enfatizzata e posta all'attenzione, anche dei più distratti, che la ripresa economica deve obbligatoriamente passare per la digitalizzazione delle istituzioni, delle imprese e dei cittadini.

La legge di riforma della Pubblica Amministrazione apporta novità in diverse materie, alcune di queste hanno aspetti che riguardano la pubblica amministrazione, l'ambiente, e la sicurezza sul lavoro: sostanzialmente la legge affida al Governo più di 15 deleghe da adottare entro termini che vanno da 90 a 180 giorni e da 12 a 18 mesi dall'entrata in vigore. Tuttavia, ci sono delle misure che sono immediatamente operative, come alcune modifiche della Legge in materia di procedimento amministrativo: definizione di un meccanismo per il silenzio-assenso tra amministrazioni statali; modifiche alla SCIA e alla cosiddetta "autotutela amministrativa", ossia l'annullamento d'ufficio degli atti amministrativi.

Dal punto di vista "digitale", al fine di garantire ai cittadini e alle imprese, il diritto di accedere a dati, documenti e servizi on line, il Governo è delegato ad adottare, uno o piu' decreti legislativi volti a modificare e integrare, anche disponendone la delegificazione, il Codice dell'amministrazione digitale - CAD (Dlgs 82/2005). In tale contesto, la Carta della cittadinanza digitale fornisce una serie di indicazioni e orientamenti che il Governo, delegato a modificare il CAD, dovrà seguire.

La legge è in vigore dal 28 agosto 2015.

Riferimento normativo: L. 7 agosto 2015, n. 124, pubblicata sulla Gazzetta Ufficiale n. 187 del 13 agosto 2015.

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Rapporto OCSE: la digitalizzazione ha rivoluzionato anche "le azioni fiscali"

L'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) ha pubblicato un rapporto che fornisce utili dettagli sulle strategie adottate dalle Amministrazioni tributarie internazionali più all'avanguardia.
La ricetta vincente risultata dal report Tax administration 2015 è la seguente: ridurre i costi, incentivare i servizi fiscali online e migliorare la tax compliance.

La riduzione dei costi è stata realizzata, nel 60% delle amministrazioni coinvolte, attraverso la riduzione del personale, e la conseguente riunificazione degli uffici periferici: ad esempio, in paesi come Portogallo, Repubblica Slovacca e Slovenia, è allo studio la creazione di un'unica Agenzia per fisco e dogane; Grecia e Lituania, stanno valutando la possibilità di accorpare la riscossione di tasse e contributi sociali.

L'elemento interdisciplinare che risulta maggiormente influente, nelle amministrazioni fiscali all'avanguardia, è la digitalizzazione. La maggioranza delle istituzioni analizzate ha intrapreso la strada della digitalizzazione, spingendo i contribuenti all'utilizzo dei servizi online rispetto ai canali tradizionali, meno efficienti e più costosi. Tra i servizi fiscali digitali, il più diffuso è l'invio della dichiarazione dei redditi, presente nel 95% dei casi esaminati. Nonostante questo, la media della spesa per lo sviluppo delle infrastrutture tecnologiche sul totale del budget a disposizione, rimane bassa, circa il 9%. A investire di più nell'Information technology sono Austria, Finlandia, Singapore e Norvegia, con circa il 25% del budget complessivo.

Fonte: Comunicato stampa Organizzazione per la cooperazione e lo sviluppo economico (OCSE) dell'11 settembre 2015

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Sistema pubblico di Identità digitale: avviato l'accreditamento dei gestori

L'Agenzia per l'Italia Digitale (AgID), con proprio comunicato stampa, annuncia di aver avviato le procedure di accreditamento per gli aspiranti Identity Provider, che saranno abilitati alla distribuzione e alla gestione di identità digitali nell'ambito del Sistema Pubblico di Identità Digitale (SPID).

Lo SPID è la nuova piattaforma che permetterà a cittadini e imprese di accedere con un'unica identità digitale, ai servizi on line della pubblica amministrazione e dei privati che vi aderiranno.

Dal momento in cui verrà ufficializzata da AgID l'iscrizione nel registro SPID del primo Identity Provider, le pubbliche amministrazioni avranno 24 mesi di tempo per adeguare i sistemi di login dei propri siti all'accesso tramite SPID.

Le sei Regioni (Piemonte, Emilia Romagna, Toscana, Liguria, Marche, Friuli Venezia Giulia), Agenzia delle Entrate, Inps e Inail, che hanno partecipato alla fase di test del sistema, permetteranno l'accesso ai propri servizi digitali tramite identità SPID già dalla fine del 2015.

Riferimenti: Comunicato stampa Agenzia per l'Italia Digitale http://www.agid.gov.it/

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Identificazione elettronica persone fisiche e giuridiche: interoperabilità obbligatoria nell'UE

L'identificazione elettronica delle persone fisiche e giuridiche non può rispondere a regole nazionali. Questo il principio di fondo che ha portato all'emanazione del presente regolamento europeo: i sistemi di identificazione elettronica adottati nell'Unione Europea devono essere in grado di "dialogare" rendendo possibile lo scambio di informazioni su soggetti fisici e giuridici.
Il presente regolamento stabilisce i requisiti tecnici e operativi al fine di garantire l'interoperabilità dei regimi di identificazione elettronica che gli Stati membri devono notificare alla Commissione UE.

Detti requisiti comprendono in particolare:
a) i requisiti tecnici minimi relativi ai livelli di garanzia e alla mappatura dei livelli di garanzia nazionali dei mezzi di identificazione elettronica forniti nell'ambito dei regimi di identificazione elettronica (Regolamento 910/2014/UE);
b) i requisiti tecnici minimi per l'interoperabilità;
c) l'insieme minimo di dati di identificazione personale che rappresentano un'unica persona fisica o giuridica;
d) le norme di sicurezza operativa comuni;
e) le disposizioni per la risoluzione delle controversie.

In vigore dal 29 settembre 2015

Riferimenti: Regolamento 2015/1501/UE pubblicato in GUUE serie L, n. 235 del 9 settembre 2015

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa

41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Il Garante europeo per la protezione dei dati ha espresso il suo parere sulla riforma per la protezione dei dati personali

CNA Brussels' Office informa che, lo scorso 27 luglio, il Garante europeo per la protezione dei dati (GEPD), Giovanni Buttarelli, ha pubblicato un suo parere sulla riforma della protezione dei dati personali e, in particolare, sull'accordo politico che il Consiglio GAI (Giustizia Affari Interni) ha raggiunto sul regolamento generale.

Il Garante europeo, in estrema sintesi, ha sostenuto che:
• il punto di partenza di ogni considerazione riguardante il trattamento dei dati dovrebbe essere sempre la "dignità" dell'essere umano; ogni trattamento deve essere sempre legale e giustificato (termini che non possono essere in antitesi);
• esaminando gli effetti della riforma sulle imprese il regolamento deve essere semplificato nel testo; la semplificazione, infatti, evita l'aumento dei costi per le imprese più piccole e diminuisce la burocrazia (le misure di sicurezza non devono essere confuse con le formalità);
• deve essere raggiunto un equilibrio tra i diritti individuali di protezione e le esigenze di business e sviluppo tecnologico.

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa

41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

La Poltel chiude 17 siti web che si spacciavano per l'Enel

Ad inizio dell'estate 2014 si era rilevato un massiccio invio di e-mail, spedite in apparenza da "Enel SpA", per mezzo delle quali si invitavano gli utenti a collegarsi ad un link, a prima vista riferibile alla società fornitrice di energia elettrica, mediante il quale sarebbe stato possibile visionare i dettagli della propria bolletta telefonica.
Il falso portale (costruito perfettamente e contenente informazioni, così come le e-mail inviate, scritte in un ottimo italiano), però, una volta cliccato, infettava irreversibilmente i pc delle ignare vittime con il famigerato malware, noto come "cryptolocker", cioè una forma di ransomware, operante dal 2013, in grado di infettare i sistemi di Windows, criptando i dati della vittima. Per la decriptazione viene richiesto il pagamento di una somma in Bitcoin (moneta virtuale non soggetta a particolari tipi di controlli da parte delle autorità monetarie).
Il famoso esperto informatico - Dott. Umberto Rapetto - nel secondo incontro informativo annuale in materia di privacy, organizzato da Cna Nazionale, aveva espressamente sconsigliato gli imprenditori, divenuti vittime del ricatto, di effettuare il pagamento richiesto perché quasi mai risolutivo del problema.
Alla fine di complesse indagini portate avanti dalla Poltel per arginare il fenomeno, il 30 luglio sono stati chiusi 17 dei falsi siti web dell'Enel (per lo più situati in Turchia e Russia).

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

I dati dell'Osservatorio CRIF confermano l'inarrestabile crescita dei furti di identità

L'Osservatorio CRIF, che identifica le caratteristiche e le tendenze del fenomeno delle frodi creditizie sulla base di informazioni e dati aggiornati annualmente, per il 2014 ha evidenziato la continua crescita delle frodi creditizie in Italia, più di 25.500, stimando una perdita economica superiore ai 171 milioni di Euro.

"Le frodi creditizie sono atti criminali realizzati mediante furto di identità (phishing, vishing, ecc.) e il successivo utilizzo illecito dei dati personali e finanziari altrui per ottenere credito o acquisire beni con l'intenzione premeditata di non rimborsare il finanziamento e non pagare il bene".
L'analisi della distribuzione delle frodi nell'anno 2014 ha evidenziato che nella maggioranza dei casi sono gli uomini, in sostanziale continuità rispetto al trend degli anni passati, a esserne colpiti (il 62,4%) e che la fascia di età maggiormente a rischio (il 25,1% del totale) è compresa tra i 41 e i 50 anni.

Il consigli forniti da Crif per difendersi da questi tipi di reati sono:
• elevare il livello di allerta e di autotutela, ad esempio ponendo la massima attenzione a ciò che viene condiviso online (mai condividere la foto del proprio cane specificandone il nome, se questo è utilizzato anche come password della casella di posta elettronica o dell'internet banking);
• usare una password diversa per ogni profilo e assicurarsi che sia a prova di violazione;
• aggiornare sistematicamente programmi e sistemi operativi perché spesso le vulnerabilità delle vecchie versioni sono utilizzate dai frodatori per installare malware, in grado di spiare e rubare le password;
• quando si decide di rivendere o scartare computer, smartphone e tablet bisogna essere certi che i dati personali in esso presenti siano stati definitivamente eliminati;
• stare attenti non solo alla tecnologia ma anche alle informazioni contenute in documenti che distrattamente vengono cestinati (meglio ricordarsi di strapparli minuziosamente o renderli sempre illeggibili).

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Approvati dall'Agenzia per l'Italia digitale i 4 regolamenti necessari per rendere operativo il Sistema Pubblico per la gestione dell'identità digitale

L'Agenzia per l'Italia Digitale, dopo un produttivo confronto con il Garante per la protezione dei dati personali sulle caratteristiche e modalità di adozione del Sistema Pubblico di Identità Digitale (SPID), ha reso noto che sono stati emanati i quattro regolamenti necessari per renderlo operativo.
Lo SPID è un sistema volto a fornire ai cittadini ed alle imprese le identità digitali necessarie per consentire il dialogo in sicurezza con le pubbliche amministrazioni.
I quattro regolamenti approvati riguardano:
- le caratteristiche del sistema pubblico per la gestione dell'identità digitale;
- i tempi e le modalità di adozione del sistema da parte delle pubbliche amministrazioni e delle imprese;
- il riuso delle identità pregresse;
- l'accreditamento dei gestori di identità digitale (quest'ultimo regolamento entra in vigore il 15 settembre 2015 data dalla quale i soggetti interessati possono presentare domanda di accreditamento all'Agenzia).

Con l'identità digitale fornita da un fornitore accreditato dall'amministrazione potranno essere:
- svolte le pratiche con le pubbliche amministrazioni e potranno essere fruiti i servizi messi a disposizione on-line dalle stesse;
- protetti i dati personali dei cittadini, molto più che con le smart card, in quanto verranno forniti al service provider solo i dati strettamente indispensabili per la specifica transazione.

Riferimento: Determinazione AgID n. 44/201528 del luglio 2015 ; Articolo 4, commi 2/4, del DPCM 24.10.2014

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Le cyber-assicurazioni, una possibile seconda linea contro il crimine informatico

Dall'ultima analisi sul cyber risk pubblicata da A.G.C.S., centro di competenza del gruppo Allianz per l'assicurazione degli affari "Large Corporate" e "Specialty", risulta che entro il 2025 il mercato assicurativo informatico arriverà a più di 20 miliardi di dollari di premi rispetto ai 2 miliardi attuali.

Questo perché in 15 anni il cyber crime da "rudimentale" è diventato un fenomeno sempre più complesso, per la crescente interconnessione di dispositivi e aziende e per la mancanza di investimenti adeguati sulla sicurezza informatica (specie in Italia). Allianz, nel suo rapporto, sottolinea che i rischi informatici si stanno ampliando; non riguardano più solo i pericoli connessi alla violazione dei dati personali, delle informazioni aziendali e della reputazione ma anche il furto della proprietà intellettuale, l'estorsione e l'interruzione di attività aziendali. La "business interruption" è probabile che nei prossimi 5/10 anni possa diventare il pericolo principale per la "cyber assicurazione", vista ormai come seconda linea difensiva per le imprese, in quanto sebbene non possa difendere le imprese dagli incidenti informatici, contribuisce a mitigarne le perdite.

Anche i prodotti assicurativi sono destinati ad articolarsi sempre più includendo:
• spese generate dalle misure rese necessarie per rispondere al verificarsi di attacchi alla rete informatica aziendale e al conseguente ripristino dei dati danneggiati o distrutti;
• perdita di entrate derivanti da malfunzionamenti cagionati dal cyber attacco;
• copertura della responsabilità civile dell'azienda assicurata nei confronti dei propri clienti/utenti e contro la violazione di dati e la pirateria informatica;
• costi legati alla comunicazione di crisi destinata a tutelare la reputazione dell'azienda.

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Per la Cassazione sono utilizzabili come prova i dati acquisiti da un computer sequestrato se le informazioni originali non sono state alterate

Dopo che in primo grado due imputati erano stati condannati dal Tribunale di Ancona per reato di frode informatica, rivelazione del contenuto di documenti segreti e accesso abusivo ad un sistema informatico unificati sotto il vincolo della continuazione alla pena di 1 anno e tre mesi di reclusione e ad una multa di 1.000 Euro, avendo gli stessi proposto gravame, in Appello erano stati assolti perché il fatto non sussiste.

Il successivo ricorso per Cassazione delle parti civili si è fondato sulla violazione di legge processuale del giudice di appello in merito all'inutilizzabilità dei risultati degli accertamenti compiuti sui documenti informatici contenuti sui supporti sequestrati. Secondo i ricorrenti "la normativa prevista dalla L. n. 48/2008 si limita ad imporre la conservazione e la non alterazione dei dati, ma non prescrive l'adozione di modalità determinate", tali atti, pertanto, non potevano definirsi irripetibili. Nel caso specifico il perito aveva dimostrato che nessun dato del supporto informatico era stato modificato.

La Cassazione ha quindi ritenuto che per i dati contenuti nel computer la riproduzione è un'operazione meramente meccanica e può essere effettuata più volte. Ha quindi annullato la sentenza della Corte d'Appello, stabilendo il rinvio ai soli effetti civili.

Riferimento: Cassazione - Seconda sezione penale - Sentenza n. 29061/2015

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Per il reato di diffusione di materiale pedopornografico non basta rinvenire file nella cartella "incoming" di eMule

Un imputato è ricorso in Cassazione contro la decisione della Corte di Appello di Milano, che lo aveva condannato per diffusione continuata di materiale pedopornografico aggravata, in base al fatto che le immagini erano state lasciate nelle cartelle "incoming" di eMule destinate alla condivisione e all'ingente quantitativo di file scaricati.

La Suprema Corte, nell'accogliere il ricorso con rinvio ad altra sezione della Corte di Appello di Milano, ha ribadito che affinché sussista il dolo del reato di cui all'art. 603 ter, comma 3, del Codice penale, occorre provare che l'imputato abbia avuto non solo la volontà di procurarsi materiale pedopornografico ma anche la specifica volontà di distribuirlo, divulgarlo, diffonderlo o pubblicizzarlo, desumibile da elementi specifici e ulteriori rispetto al mero uso di file sharing o dal dato quantitativo del materiale scaricato (in particolare i giudici di merito avrebbero dovuto avviare specifiche indagini volte ad accertare in concreto se la volontà dell'imputato era finalizzata al semplice approvvigionamento o anche alla diffusione dei file pedopornografici).

Riferimento: Cassazione - Terza Sezione penale - Sentenza n. 30465 del 15.7.2015 (ud. 12 maggio 2015)

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa

41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

La diffamazione può consentire l'oscuramento di un blog o di un forum

Il quotidiano on-line è assimilato a quello cartaceo e non può essere sottoposto a sequestro preventivo, mediante oscuramento, per un articolo passibile di diffamazione.

Requisiti caratterizzanti un quotidiano on-line sono: l'essere un prodotto editoriale con una propria testata identificativa; la finalità di raccogliere, commentare e criticare notizie di attualità; la diffusione con regolarità in rete; l'avere un direttore responsabile giornalista professionista o pubblicista; la registrazione presso il tribunale del luogo in cui ha sede la redazione; l'avere un hosting provider che ne è lo stampatore di cui rende noti i dati identificativi ed un editore iscritto al registro degli operatori della comunicazione.
Le garanzie costituzionali per la stampa non possono però essere applicate a blog, forum o siti generici che appartengono all'ambito "vario ed eterogeneo della diffusione di notizie in rete".

Così hanno stabilito le Sezioni unite penali della Cassazione, affermando che blog, forum e social network costituiscono certamente espressione del diritto di libera manifestazione del pensiero (art. 21 della Costituzione), ma rientrano nelle risorse telematiche ed informatiche che sono equiparate a "cose", cui non è attribuibile la tutela prevista per la stampa e quindi sono soggetti a sequestro cautelare preventivo quando esista il "fumus" della diffamazione.

Riferimento: Cassazione, Sezioni unite penali, Sentenza n. 31022 del 17.7.2015

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Massivo attacco degli hacker contro il sito di "incontri discreti tra persone sposate" AshleyMadison.com

A fine luglio di quest'anno al sito canadese AshleyMadison.com (lo stesso è capitato ai siti CougarLife.com e EstablishedMen.com) è stato mosso un attacco "puritano" degli hacker di Impact Team volto a smascherare le persone sposate, che ad esso hanno aderito, e a pubblicarne i loro dati, circa 10 gigabyte, sul dark web volti ad esporli a pubblico ludibrio.

Per quanto non si possa non rilevare una deprecabile scarsa attenzione alla sicurezza dei dati degli utenti da parte dei gestori del sito di appuntamenti – come emerge chiaramente dalle pubblicazione delle loro e-mail interne - è davvero difficile provare un minimo di comprensione per il comportamento di hacker che sembrano non curarsi delle possibili conseguenze del loro gesto, dalle liti ai rapporti familiari distrutti, dai ricatti alla presunzione di qualcuno di potersi ergere a giudice morale ed infine a presunti casi di suicidio di cui si è avuta notizia sui quotidiani.

Questa volta gli hacker hanno preso di mira proprio le preferenze sessuali, a prescindere dalla colpevolezza o dalla innocenza dei soggetti, cumulativamente definiti "pezzi di m… traditori", per i quali non può esservi un diritto alla riservatezza. Di questi soggetti sono stati messi a nudo già 37 milioni di dati (nomi, cognomi, indirizzi e-mail, carte di credito, password).

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Il Garante privacy ha rilevato gravi violazioni della privacy dei bambini da parte di siti e app

Il Garante italiano per la protezione dei dati personali ha reso noti i risultati dell'indagine svolta in collaborazione con altre ventotto Autorità internazionali del Global Privacy Enforcement Network (GPEN), in occasione del "Privacy Sweep 2015", su 22 app e 13 siti utilizzati dai bambini italiani tra gli 8 e 13 anni.
Dei 35 casi analizzati (appartenenti al settore educational, al mondo dei giochi, a servizi on-line offerti da canali televisivi per l'infanzia, ai social network), 21 hanno evidenziato gravi profili di rischio e, per 8 di questi, sono previste specifiche attività ispettive dell'Authority italiana.

I risultati dell'indagine possono così riassumersi:
• in 30 casi vengono raccolti dati personali; in 25 casi si è riscontrato l'obbligo di registrarsi inserendo almeno l'indirizzo di posta elettronica; in 20 casi è richiesto il proprio nome; in 13 casi si deve consentire l'accesso a foto e video presenti sullo smartphone, sul tablet o sul pc;
• 19 tra siti e app registrano l'indirizzo IP; 18 l'identificativo unico dell'utente; 11 richiedono la geolocalizzazione del dispositivo utilizzato dal bambino;
• in 23 casi è prevista la condivisione con altri soggetti dei dati personali raccolti;
• 23 tra siti e app includono banner pubblicitari di terze parti (talvolta anche non attinenti al mondo dell'infanzia). In 22 casi il minore può essere reindirizzato fuori dal sito/app che sta utilizzando. Alcune app consentono al bambino di procedere direttamente all'acquisto di prodotti e servizi (acquisti "in app");
• sono pochi i siti e le app in cui è presente un'informativa privacy chiara e completa, o che consentono un utilizzo senza la richiesta di dati personali. Limitati sono anche gli strumenti (es. parental control, chat preimpostate) adottati per aiutare i bambini a non diffondere, anche involontariamente, i propri dati personali.

Il poco confortante panorama italiano è però in linea con i risultati acquisiti a livello globale per i quali:
• Il 67% dei siti/delle app esaminati raccoglie informazioni personali su minori;
• Solo il 31% dei siti/delle app offre meccanismi efficaci per limitare la raccolta di dati personali di minori.
• Il 50% dei siti/delle app fornisce dati personali a soggetti terzi;
• Il 22% dei siti/delle app offre la possibilità ai minori di indicare il proprio numero telefonico; il 23% consente loro di mettere a disposizione foto o video; il 71% non offre strumenti per cancellare agevolmente le informazioni contenute negli account;
• Il 58% dei siti/delle app offre al minore la possibilità di essere reindirizzato verso un altro sito;
Infine, solo il 24% dei siti/delle app promuove il coinvolgimento dei genitori.
Da alcuni siti ed app provengono però anche buone prassi riguardanti l'offerta di controlli efficaci (cruscotti riservati all'intervento dei genitori, avatar e/o ID utenti predefiniti per impedire che un minore riveli senza volerlo informazioni personali) e di chat che permettono ai minori di selezionare parole e frasi solo da elenchi predefiniti, o la visualizzazione di alert preventivi volti ad evitare che il minore inserisca dati personali non necessari.

Riferimento: Comunicato stampa del Garante privacy del 7 settembre 2015

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Telegram e il vantaggio competitivo di proteggere la privacy

Telegram è una app di messaggistica, rilasciata dalla società Telegram LLC, che in soli 8 mesi ha decuplicato la mole dei messaggi gestiti. A fine agosto, ha toccato i 10 miliardi (cioè un terzo di quelli distribuiti da Whatsapp). Punti di forza dell'applicazione, basata su cloud e fortemente criptata, sono la possibilità di scambiare file di grandi dimensioni (fino a 1,5 GB) e, soprattutto, la possibilità di effettuare comunicazioni cifrate.
La gestione riservata dei dati personali è, infatti alla base, del pensiero dei suoi ideatori, Pavel e Nikolai Durov (che hanno fondato Telgram LLC nel 2013). Sul sito di Telegram, infatti, si legge: "… le grandi compagnie di internet come Facebook o Google negli ultimi anni hanno effettivamente trascurato il discorso privacy. I loro manager sono riusciti a convincere il pubblico che le migliori soluzioni per la privacy sono funzionalità superficiali che ti permettono di nascondere il tuo stato online, i tuoi post pubblici o le tue foto profilo dalle persone attorno a te. Aggiungere queste funzionalità superficiali permette alle compagnie di calmare il pubblico e di non cambiare nulla nel modo in cui inoltrano dati privati ai manager e a terzi. Noi di Telegram crediamo che i due più importanti componenti della privacy su internet dovrebbero invece essere: 1.proteggere le tue conversazioni private dalla curiosità di terzi, come funzionari, impiegati, ecc.; 2. proteggere i tuoi dati personali da terzi come manager, pubblicitari, ecc. …".

La chat segreta (che Telegram offre accanto alla chat normale), utilizzando una cifratura "end-to-end", sta avendo un grande seguito, specie tra i giovani (qualche settimana fa era la più scaricata in 46 paesi del mondo), consentendo ai propri utenti di impostare una scadenza per i messaggi che vengono mandati a qualcuno ben sapendo che, alla data stabilita, questi spariranno definitivamente.
Mentre il Parlamento europeo in questi anni è sembrato timoroso nell'approvare il Regolamento sul trattamento dei dati personali, quasi a non voler scontentare gli interessi della lobby informatica di oltre-oceano, una nuova generazione di europei pare abbia incominciato a riconoscere il valore della tutela della propria privacy.

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Il Garante privacy ha predisposto consigli flash su come tutelare la privacy con buone password

Dopo che il Garante della protezione dei dati personali, nei mesi scorsi, aveva pubblicato sul suo sito istituzionale due "consigli flash", schede riassuntive che offrono spunti e orientamenti di base per tutelare i propri dati personali nella vita di tutti i giorni (con particolare attenzione all'uso delle nuove tecnologie),
intitolati "Social privacy, Connetti la testa"" e "Fatti smart", recentemente ha reso disponibile una terza scheda dal titolo "Consigli flash per tutelare la tua privacy con buone password",

La scheda si articola in 4 punti: 1) come è fatta una buona password, 2) utilizza password diverse per account diversi (e-mail, social network, etc), 3) conserva con cura le password, 3) prova ad usare software "gestori di password", offrendo dei suggerimenti utili per impostare e conservare le password utilizzate per gli account informatici sia in ambito lavorativo sia in ambito privato.

In un'epoca in cui il crimine informatico si sta sempre di più diffondendo, non è male ricordare che una buona password dovrebbe:
• essere abbastanza lunga (almeno 8 caratteri);
• contenere caratteri di almeno 3 diverse tipologie: lettere maiuscole, minuscole, numeri, caratteri speciali (punti; trattino, underscore, etc.);
• non contenere riferimenti personali facili da individuare (nome, cognome, data di nascita, nome dei propri figli o dei propri animali da compagnia, etc.);
• essere periodicamente cambiata, almeno per i profili più importanti o quelli utilizzati più spesso (e-mail, e-banking, social network, etc.).

Comunicazione e Terziario Avanzato
Fotografia – Grafica - Informatica
Sede Nazionale
00162 Roma – Piazza M. Armellini, 9/A
Tel. (06) 441881 – 44188 269
Fax (06) 44249515 - e-mail: comunicazione@cna.it

interpreta srl
analisi applicata della normativa
41122 Modena - Via Malavolti, 5
tel. 059 418376
fax 059 418398
e-mail info@interpreta.it
www.cnainterpreta.it

Per il Garante privacy le intercettazioni da remoto effettuate senza sufficienti garanzie privacy diventano prove illegittime

Il Garante italiano, dando notizia sul proprio sito istituzionale di un suo intervento sul quotidiano "Il Messaggero", ha evidenziato che la giurisprudenza del Tribunale costituzionale portoghese e della Cassazione italiana confermano le preoccupazioni, a suo tempo espresse sulla vicenda Hacking Team, riguardanti l'inutilizzabilità degli elementi di prova ottenuti con tecniche investigative atipiche e non circondate da sufficienti garanzie volte ad assicurare l'equilibrio tra libertà e sicurezza, diritto e tecnologia, privacy e giustizia/intelligence.

Il Tribunale costituzionale portoghese, infatti, ha dichiarato incostituzionale le legge anti-terrorismo del proprio Stato, ad un solo mese dalla sua approvazione, nella parte in cui autorizza gli organi di intelligence ad acquisire tabulati telefonici e telematici in base a una mera autorizzazione giudiziale (come in Italia); al contrario sarebbero necessarie quelle maggiori garanzie che solo un processo penale può offrire. Per motivare la sua decisione il Tribunale ha richiamato la sentenza con cui, un anno fa, la Corte di giustizia europea ha annullato la direttiva sulla conservazione dei dati di traffico per violazione del principio di proporzionalità tra privacy ed esigenze investigative e la possibilità di limitare il diritto all'intangibilità della sfera privata nella misura strettamente indispensabile, solo in presenza di esigenze investigative effettivamente accertate, da parte di un organo terzo.

La Cassazione italiana, inoltre, il 26 giugno scorso, ha stabilito essere illegittime, pertanto inutilizzabili, le intercettazioni ambientali realizzate mediante immissione di virus informatici in uno smartphone, capaci di attivare in ogni momento la videocamera del telefono. Tale tecnica investigativa, consentendo un controllo totale dell'indagato (in ogni luogo e contesto), sarebbe talmente pervasiva da non avere più alcun limite né possibilità di riscontro effettivo.

La vicenda Hacking Team, pertanto dimostra che:
- i dispositivi utilizzati per le intercettazioni da remoto, perfettamente in grado di "concentrare", in un unico atto, una pluralità di strumenti investigativi (perquisizioni del pc, pedinamenti con satellitare, intercettazioni, acquisizioni di tabulati) e di eliminare le tracce delle operazioni effettuate (anche alterando i dati acquisiti facendo saltare tutte le garanzie stabilite dal codice di rito a tutela dell'indagato) non possono essere utilizzati indiscriminatamente;
- l'authority aveva ben operato nel febbraio chiedendo lo stralcio all'emendamento proposto
al decreto-legge anti-terrorismo che avrebbe legittimato le intercettazioni da remoto, in assenza di garanzie adeguate;
- una tecnologia non adeguatamente regolamentata non sviluppa la libertà ma, al contrario, la insidia perché già "la sola percezione di poter essere continuamente controllati è essa stessa perdita di libertà"