Il Diritto alla privacy in ambito europeo ed internazionale

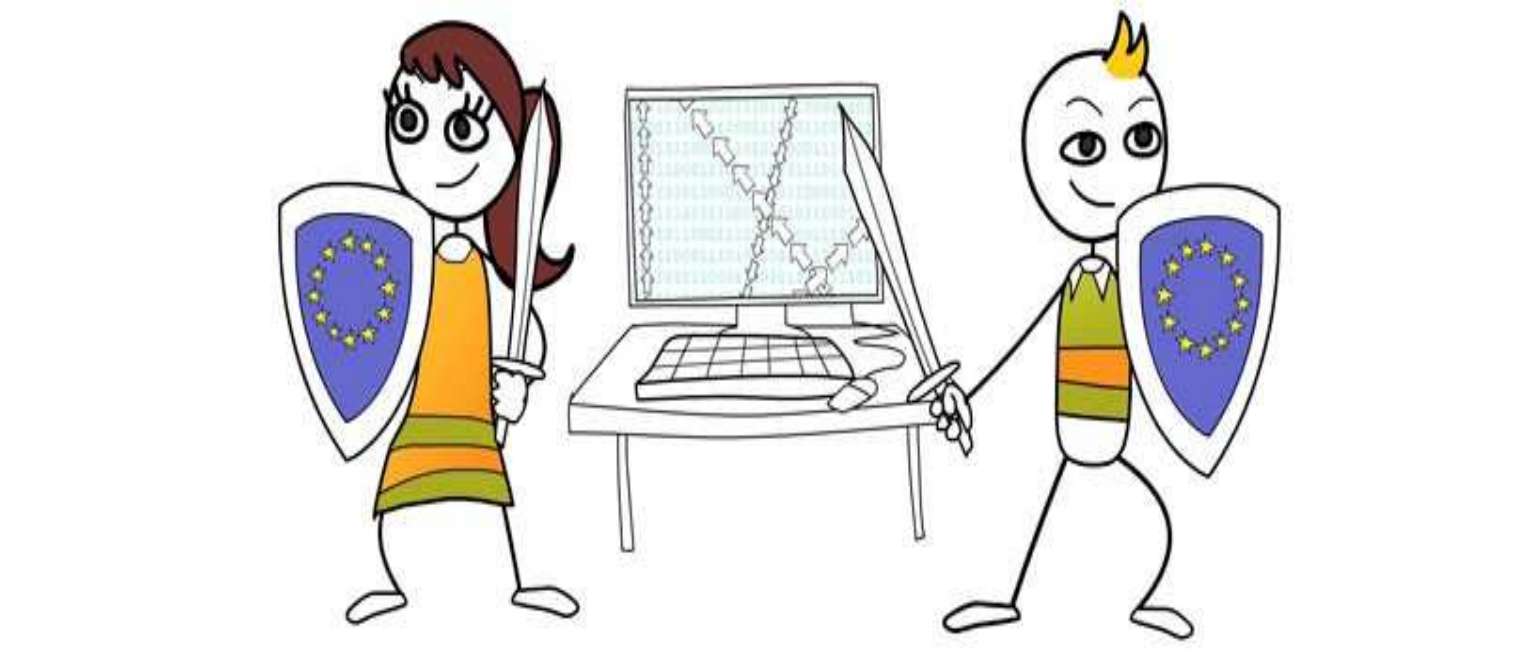
Avv. Felix Hofer, Firenze – www.hltlaw.it

Articolazione del contributo:

- 1.- Social networks e tutela fornita dall'Unione Europea.
- 2.- Elementi necessari per una difesa efficace della privacy - Cenni sulla prova informatica. *
- 3.- Studio della giurisprudenza rilevante. *

** Ringrazio la collega Angela Tripodi per la collaborazione*

1.- Social networks e tutela fornita dall'Unione Europea.



1.1. Contesto e individuazione problemi:

Contesto:

1.1. Contesto e individuazione problemi:

Contesto:

Qualche numero su FB (e poi ci sono YouTube, Twitter, LinkedIn, Instagram, WhatsApp, Messenger, ecc.):

Mondo: 2 mlrd. utenti/mese giu. 2017 (845 mil. feb. 2012)

Europa: 343 mil. utenti/mese giu. 2017

Social media in **Italia**:

- 31 mil. utenti attivi (= +50% popolazione)
- 74% accede a FB una volta al giorno (55% media mondiale)
- Ore permanenza/mese su FB: 12 (2H YouTube).

Ricerca risorse umane:

Non più

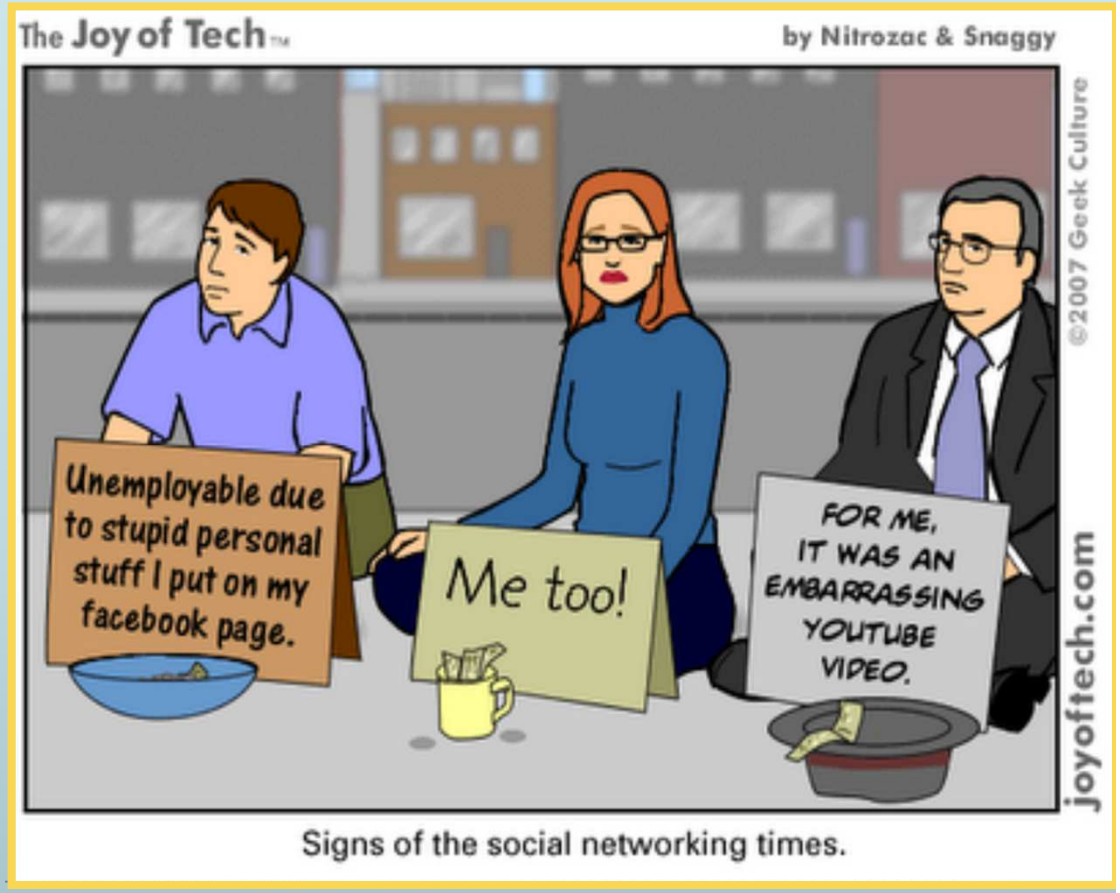
Sì

1.1. Ricerca risorse umane:

- 70% datori lavoro esamina profili individuali sui SM/ reputaz. online candidati.

- Rifiuto per:

- Foto provocatorie 46%
- Assunz. alcool, droga 40%
- Commenti negativi 34%
- Scarsa cap. comm. 30%
- Commenti discrimin. 29%



Signs of the social networking times.

1.1. Ma Anche Dopo Assunzione:

- **Tribunale Ivrea, Sez. Lavoro, 28-01-2015:**

Licenziamento giustificato per commenti offensivi per datore lavoro e colleghi postati su FB.

- **Tribunale Milano, Sez. Lavoro, 1-08-2014:**

Legittimo licenziamento per pubblicazione su profilo pubblico di FB di foto prese su posto di lavoro e commenti offensivi per reputazione azienda.

- ***Tribunale Bergamo, Sez. Lavoro, 14 settembre 2016:***

Licenziamento anche per fatti extra contesto lavoro, se comunque incidenti e tali da far venire meno interesse datore di lavoro.

1.1. *segue* Dopo Assunzione:

- ***Anche Garante ritiene legittimo l'uso – per fini disciplinari - di ogni manifestazione "tracciata" sui social network da parte del proprio dipendente, se non vi siano filtri all'accesso.***

- **Corte di Cassazione, 27-05-2015 n. 10955:**

Licenziamento per uso SN - giustificato creazione falso profilo per accertare ripetute e prolungate conversazioni tel. private e utilizzo tablet per navigazione FB sul posto di lavoro (trascurando le esigenze di sicurezza e prevenzione dell'impianto produttivo). Controllo difensivo occulto legittimo.

Rischi: Minorenni

Rischi: Minorenni

Indagine condotta in Italia

Foto con nudi int. o parz. o con contenuto sess'le esplicito:

- 4 su 100 bambini nella fascia di età tra i 12 e 14 anni,

- 8 su 100 ragazzi tra i 15 e 17 anni.

Abitudini 453 soggetti intervistati (età 12 – 17):

- 43%: ha caricato messaggi con riferimenti sessuali,
- 43%: ha reso disponibili informazioni pers. agli 'amici' on-line,
- 41%: ha visto contenuti sessualmente espliciti,
- 40%: ha fornito proprio numero di cell. a 'contatti' su Internet,
- 22%: ha intrapreso 'relazioni intime' con sogg. reperiti on-line

Minorenni: i teenagers

Indagine 2016 condotta negli Stati Uniti:

- + 75% sono sui social media
- 91% carica foto personali
- 71% rivela nome propria scuola
- 53% indica proprio indirizzo e-mail
- 20% espone il proprio numero di cellulare

Conforta una asserita maggiore consapevolezza?

- 60% scelgono il profilo 'solo per gli amici'
- 56% trovano facili i 'privacy settings' dei SM
- 67% 'nascondono' att. SM, 10% capaci aggirare parent. cont.

Segue Rischi: Conclusioni

Recente indagine di *Save the Children*:

- Oltre 30% minorenni intervistati nasconde attività online ai genitori,
- Oltre 80% genitori ritiene 'al sicuro da pericoli' minorenni nelle loro stanze collegati a Internet

MA

Se in una nota pubblicità per gioielli ***«un diamante è per sempre»***, lo stesso vale per un post su Internet!

1.2. Sforzi per arginare i rischi

Approccio UE – Strategie di persuasione: "Educazione-Informazione-Collaborazione"

1999: Commissione UE vara ***Safer Internet Programme - SIP***

2004: Nasce ***Insafe Network*** per promuovere SIP

OGGI: *Insafe* e *Inhope* gestiscono ***Safer Internet Centres – SIC*** (nei paesi membri UE + Islanda, Norvegia e Russia) con:

- Awareness centre per educazione/formazione
- Helplines per info., cons. e assist. su come gestire contenuti e comportamenti pericolosi o rischiosi,
- Hotlines per raccogliere segnalazioni (anche anonime) da passare ad Autorità competenti
- Youth panels = piattaforme x scambio esperienze e conoscenze

Dal **2005** *Insafe* organizza ogni anno (a febbraio) il ***Safer Internet Day*** (iniziativa oggi ripresa in più di 120 paesi in 6 continenti)

Cronologia iniziative significanti

2009 - Acc. Pan-Europeo *"Safer Social Networking Principles for the EU"* tra 20 providers per:

- ***Formaz.*** su esigenze di sicurezza e uso accettabile
- ***Servizi adeguati*** a età utenti,
- ***Selezione impostazioni*** per utenti,
- ***Facilità segnalaz***. comport. illeciti e contenuti inapprop.,
- ***Reazione tempestiva*** a tali segnalazioni,
- ***Educazione utenti*** su approccio sicuro al cari'mento di informazioni e dati personali,
- ***Strumenti per bloccare*** comportamenti e/o contenuti illeciti

segue Acc. Pan-Europeo "Safer Social Networking Principles"

Soggetti da coinvolgere:

Genitori, insegnanti, educatori, assistenti infanzia: → dialogo continuo e informaz. adeguata

Governi e Amm. ni Pubbl.: → iniziative legislat., di prevenz. repress. e collaboraz.internaz.

Autorità controllo e FF.PP: → int.ti invest., di prevenzione, repress. e collab. reciproca (anche internaz.),

Società Civile (e sue org.): → collaboraz. costante con tutti interlocutori interessati

Utenti: → uso di misure di sicurezza, comportamenti adeguati, osserv. regole condotta.

Linee Guida Gruppo Lavoro ex Art. 29 (12 Giugno 2009 – WP 163)

- Providers di servizi di SN **soggetti** ai principi e obblighi Direttive UE sul trattamento di dati personali.
- **Osservanza principi** dell'uso consono e proporzionato, della conservazione solo per il periodo necessario.
- **Ottemperanza a prescrizioni** specifiche:
  informativa utenti, indicazioni su rischi, offerta facili impostazioni di preservazione privacy, protezione dei minorenni, rispetto diritti dei terzi, cancellazione account abbandonati,
- **Garanzia diritti utenti** anche attraverso facili procedure di obiezione e utilizzo di pseudonimi,
- **Tecniche invasive** di *DM* (es. 'commercializzazione comportamentale, contestuale e segmentata') devono rispettare le prescrizioni a tutela della privacy degli utenti

Verifica 2010 Comm. UE Soc. Informa. circa efficacia accordo *SSNP* del 2009

Progresso quanto adozione misure di sicurezza, linee guida per utenti, indicazioni rischi per minorenni on-line,

MA

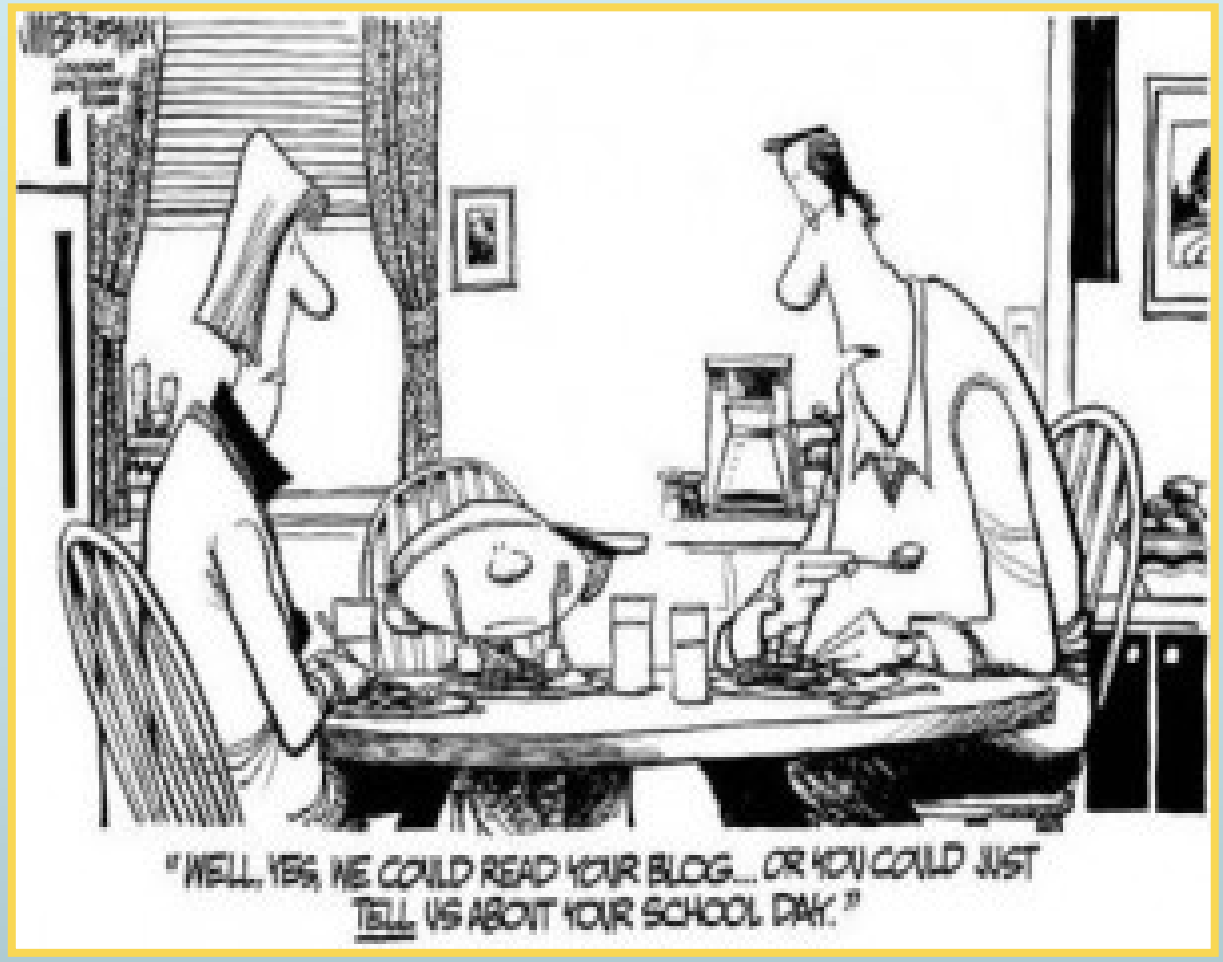
in generale NON ancora soddisfacente, poiché:

- Solo nel 50% dei casi ai motori di ricerca è impedito acquisire profili di minorenni,

- Solo in 9 casi trovati adeguati sistemi per raccogliere ed evadere esposti/richieste di aiuto utenti minorenni,

- Profili minorenni visibili solo agli 'amici' in meno del 50% dei casi

Febbraio 2010: Iniziativa *"Think B4 U Post"*



«Think Before u Post»

OBIETTIVI:

- **Spiegare** i rischi di IM e Profile Sharing,

- **Creare** consapevolezza circa i pericoli nella condivisione di profili, dati e informaz. pers., foto, video, diari, musica, blogs,

- **Avvertire** circa possibilità di sfruttamenti a fini sessuali,

- **Fornire** indicazioni su comportamenti corretti e accorti nel mondo online,

- **Sollecitare** denunce di comportamenti sospetti.

Interventi di regolamentazione
Risoluzione Strasburgo 2008 Garanti P'cy

Dieci regole per il rispetto privacy sui SN:

-1 Attenzione a cosa e a quanto pubblicare,
-2 Rispetto per la privacy degli altri,
-3 Controllo dei contenuti presenti che ci riguardano,
-4 Mirare a impostaz. di default atte a garantire sufficiente privacy,
-5 Potenziare misure di sicurezza dei sistemi,
-6 Garantire diritto di accesso per modifiche a dati presenti,
-7 Assicurare accesso per recesso e cancellazioni profili,
-8 Consentire l'utilizzo di pseudonimi,
-9 Prevenire accessi non autorizzati di terzi,
-10 Profilaz. e monitor. utenti solo previa inform. e consenso espresso.

Il Gruppo di Lavoro ex Articolo 29

Istituito da Direttiva UE n. 95/46 = organismo consultivo e indipendente, composto da un rappresentante Garanti Privacy designato da ciascuno Stato membro, dal GEPD (Garante europeo) e da un rappresentante della Commissione.

Il Gruppo di Lavoro ex Articolo 29

2008 Parere n. 1 (WP 148): le norme delle Direttive Privacy si applicano quando il MdR:

- dispone di uno 'stabilimento' sul territorio di stato membro,
- fa uso di 'strumenti' nel territorio di stato membro (salvo..)

2009 Parere n. 5 (WP 163): le tecniche di commercializz. soggette alle prescrizioni delle Direttiva Privacy

2011 Parere n. 13 (WP 185): idem per servizi di geo-localizzazione

Misure contro il Cyberbullismo

Legge 29-05-2017 n. 71

Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo.

- **Art. 7: Prevede il ricorso all'ammonimento per reati di cui agli artt. 594, 595 e 612 cod. pen. e 167 del Codice Privacy, *«se commessi, mediante la rete internet, da minorenni di età superiore agli anni quattordici nei confronti di altro minorenne».***

- **Art. 2: consente di *«inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento».***

Uno sguardo in avanti

- **La Proposta di Regolamento sulla ePrivacy**
- **Il Regolamento generale 679/2016 sul trattamento di dati personali**

Ancora il GdL ex Art. 29

2017 Parere n.1 (WP 247): sulla proposta di Reg'to *ePrivacy*.

Concorda su iniziativa ma individua criticità:

- Tracciamento della posizione dei terminali
  - ° solo se consenso o anonimi'one (+ standards tecnici),
- Analisi di contenuti e di 'metadata'
  - ° solo se consenso mittente **e** destinatari,
- Terminali e software
  - ° devono essere dotati di impostaz. di protez. by default,
- Consenso obbligato per utilizzo servizi ('tracking walls)
  - ° divieto assoluto.

Ancora il GdL ex Art. 29

2017 Parere n.2 (WP 249): trattamento dati e rapp'to di lavoro

- nel contesto della ricerca di risorse umane
- tramite monitoraggio delle comun'zioni elett. al posto di lavoro
- tramite monitoraggio comun'zioni al di fuori posto di lavoro
- per verifica delle presenze dei dipendenti
- attraverso sistemi di monitoraggio/video-sorveglianza
- attraverso verifica uso veicoli di servizio
- con rivelazione dati dei dipendenti a soggetti terzi
- con trasferimento transnaz. dati sensibili dipendenti (es. salute)

Consenso **non sufficiente** in assenza di 'interesse qualificato' + rispetto principi di proporzionalità e di uso minimale.

Ancora il GdL ex Art. 29:

2017 Linee Guida (WP 250) rispetto a obbligo di notifica (ex Reg. 679/2016) delle **violazioni della riservatezza** dei dati personali (accesso accidentale non autorizzato, perdita di dati, alterazione accidentale di dati).

2017 Linee Guida (WP 251) sul **diritto** (ex Reg. 679/2016) **di non essere sottoposto a una decisione** basata unicamente sul trattamento automatizzato, compresa la profilazione.

2017 Linee Guida (WP 259) sul **consenso** (ex Reg. 679/2016) e su come dimostrare l'averlo ottenuto (vale anche per obbligo di informativa).

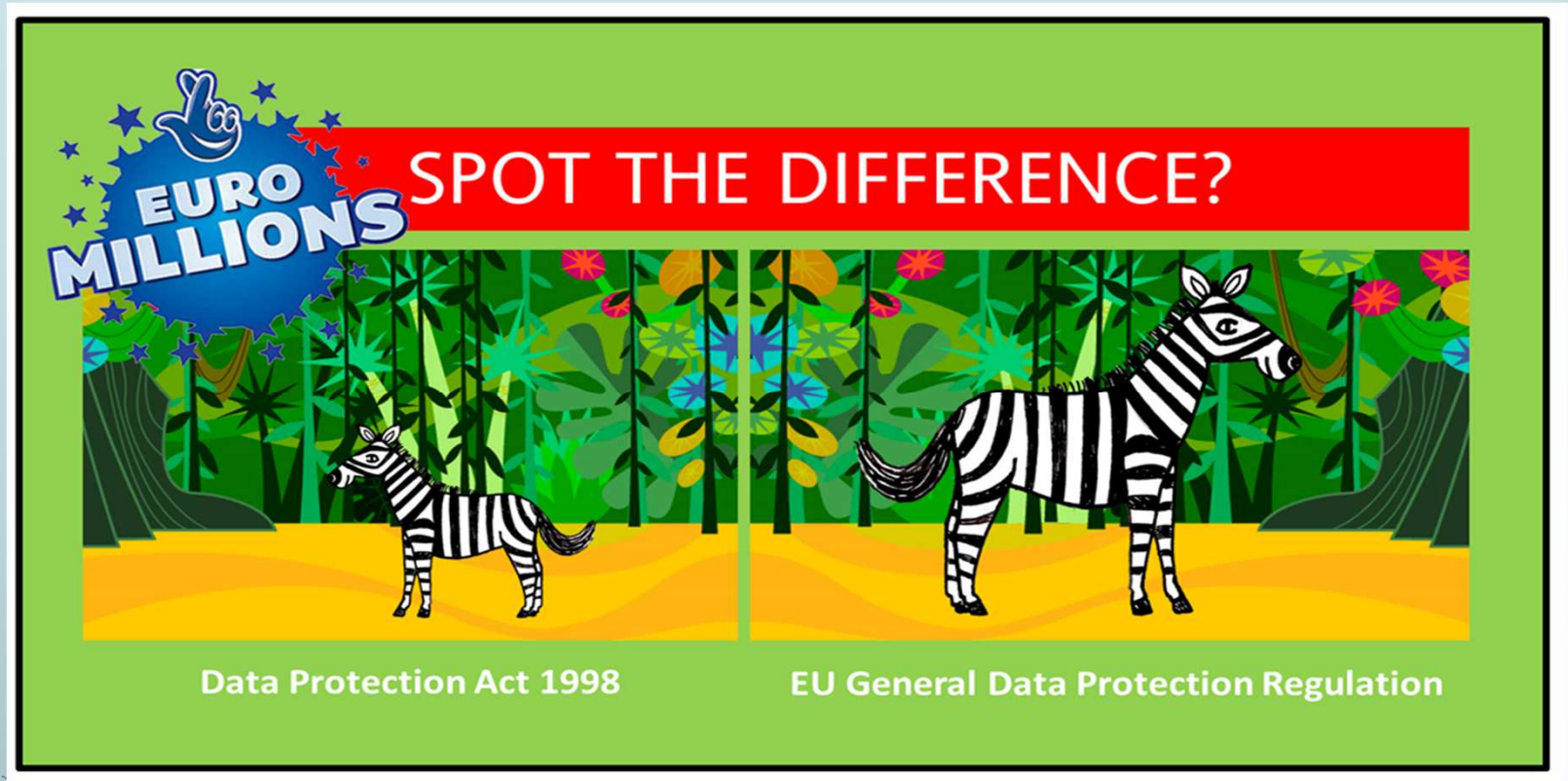
La Consapevolezza Odierna? Carente!

Secondo rapporto SWEEP 2017 (indagine su settori dei vendita al dettaglio, finanza, banche, viaggi, social network, giochi d'azzardo, istruzione, sanità):

- **Informative** generiche e imprecise
- Senza indicazioni circa eventuale comunicazione dati
- Siti e apps **carenti di spiegazioni** su uso dati
- Zero informazioni circa luogo di conservaz. e misure sicur'za
- **Solo 50%** informative spiegaz. su diritto di verifica e accesso
- Siti per servizi internaz. ignorano normativa applicabile
- Piattaforme di e-commerce **senza info** su attività espletata.

Realtà ancora lontana dal passaggio

verso una ***'cultura della privacy'***, pilastro del Regolamento Europeo n. 679/2016. Ancora dominante cultura della ***«reazione al danno»*.**



2.- Difesa efficace della privacy – Cenni sulla prova informatica.

2.1.- Misure preventive

2.2.- Reazioni a posteriori

2.1.- Misure preventive – Art. 32/1 Reg.

Sicurezza trattamento deve considerare:

- ***Stato dell'arte* - *Costi di attuazione***
- ***Natura – Contesto – Oggetto – Finalità***
- ***Probabilità e gravità rischio per diritti e libertà soggetti***

2.1.- Misure preventive – Art. 32/1 Reg.

Misure tecniche e organizzative capaci di garantire livello di sicurezza adeguato al rischio, incluse:

- ***Pseudonimizzazione – criptazione dati***
- ***Garanzie di riservatezza, integrità, disponibilità e resilienza sistemi e servizi di trattamento***
- ***Possibilità tempestivo ripristino disponibilità e accesso in caso di incidente fisico o tecnico***
- ***Procedure per test di efficienza/efficacia misure tecniche e organizzative adottate.***

2.2.- Strumenti per reazioni ex post

Intervento diretto:

Interpello rivolto dal soggetto interessato al titolare – responsabile - incaricato del trattamento (art.t 15/1/e [e segg.] del Reg. 679/2016) per opporsi al trattamento o per chiedere cancellazione, rettifica o limitazione.

2.2.- Strumenti per reazioni ex post

Tutela (alternative) amministrativa

Oggi - Codice Privacy (art. 141):

- ***Reclamo*** (per violazione disciplina trattamento)
- ***Segnalazione*** (per sollecitare controllo Garante)
- ***Ricorso*** (per far valere diritti ex art. 7 CP).

Domani – Regolamento (artt. 57 e 77):

Autorità di controllo stato di residenza tratta i ***reclami.***

2.2.- Tutela amministrativa: Poteri Garante

Codice Privacy:

- Provvisoriamente (art. 150/1):

- *Blocco dati o sospensione trattamento.*

- In via definitiva (art. 150/2):

- dispone cessaz. comportamento illegittimo, con misure di tutela interessati e assegnaz. termine di adozione.

2.2.- Tutela amministrativa: Poteri Garante

Sanzioni ex Codice Privacy

- **Carenze informative (Art. 161):**
  - **da 6.000 a 36.000 Euro**
- **Cessione irregolare (Art. 162/1):**
  - **da 10.000 a 60.000 Euro**
- **Rivelaz. stato salute (162/2):**
  - **da 1.000 a 6.000 Euro**
- **Omesse misure sicurezza:**
  - **da 10.000 a 120.000**
- **Mancata com. violaz. Garante:**
  - **da 25.000 a 150.000**

2.2.- Tutela amministrativa: Poteri Garante

segue Sanzioni ex Codice Privacy

(Artt. 163 e 164)

- Mancata comunicazione violaz. a interessati:

- da 150 a 1.000 per ciascun sogg. colpito (entro massimo 5% volume affari trasgressore)

- Omesse notifica a Garante:

- da 20.000 a 120.000

- Omesse info./esibiz. a Garante:

- da 10.000 a 60.000

2.2.- Tutela amministrativa: Poteri Garante

segue **Sanzioni ex Codice Privacy (Art. 164-bis)**

- Violazioni di minore gravità:

- sanzione ridotta a 2 / 5

- Ipotesi aggravate:

- sanzione aumentata a doppio (o quadruplo)

- Cumulo violazioni:

- da 50.000 a 300.000 Euro

- Sanzione accessoria (Art. 165):

- pubblicazione provvedimento Garante.

2.2.- Tutela amministrativa: Poteri Garante

Regolamento n. 679/2016

Autorità Controllo applica sanzioni amm. pecuniarie ***"effettive, proporzionate e dissuasive"*** (Art. 83/1) e le adatta al caso specifico tenendo conto dei segg. aspetti della violazione: ***natura, gravità, durata, carattere doloso o colposo, misure adottate, grado di responsabilità, precedent, categorie dati, grado di cooperazione con A.C., attenuanti o aggravanti***.

Sanzione pecuniaria:

- da 10 mill. Euro a 2% fatt. mondiale (artt. 8, 11, 25-37, 42, 43)
- da 20 mill. Euro a 4% fatt. mondiale (art, 5,6,7, 9, 12-22, 44-49).

2.2.- Strumenti per reazioni ex post

Tutela civile

Artt. 11 e 15 CP:

- Inutilizzabilità dati trattati illecitamente
- Obbligo risarcimento danni (anche non patrimoniali)

Art. 82 Reg.:

Obbligo di risarcimento danni

(sia materiali che immateriali)

Ovviamente:

Possibilità tutela d'urgenza (ex art. 700 c.p.c.)

2.2. Il profilo risarcitorio.

- Cass. civ. Sez. I, n. 1931/2017: ***Danno da esercizio attività pericolosa (ex art. 2050 cod.civ.) sempre da provare quanto a esistenza e nesso causale.***

- Cass. Civ. Sez. I, n. 3311/2017: ***Per risarcimento danno non patrim. ex art. 15 DLgs. non sufficiente accertamento violazione norme, ma occorre verifica gravità lesione e serietà pregiudizio.***

- CEDU, Sez. I, 1-07-2010 (Korolev c/ Russia): ***Irricevibile ricorso, difetta 'pregiudizio significativo' (nella specie meno di 1 Euro), concetto che si sottrae a 'definizione esaustiva', ma richiede almeno un 'livello minimo di serietà' con valutazione circostanze del caso insieme a percezione soggettiva ricorrente e elementi oggettivi.***

2.2.- Strumenti per reazioni ex post

Tutela penale

Artt. 167-172 CP:

Art. 167 -Trattamento illecito per profitto o per recare danni:

- reclusione da 6 a 18 mesi
- reclusione da 6 a 24 mesi (se communicaz. o diffusione)
- reclusione da 1 a 3 anni.

Art. 168 – False dichiaraz. o notifiche a Garante:

- reclusione da 6 mesi a 3 anni.

Art. 169 – Omissione misure sicurezza:

- arresto fino a 2 anni.

Art. 170 – Inosservanza provv. Garante;

- reclusione da 3 mesi a 2 anni.

2.- Cenni sulla prova informatica.

Base normativa: Codice Privacy

Art. 11/2: ***«I dati personali trattati in violazione della disciplina ……..non possono essere utilizzati»***

Art. 24/f: Trattamento senza consenso «per far valere o difendere un diritto in sede giudiziaria»

Art. 160/6: ***«La validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale»***

2.- Cenni sulla prova informatica.

La rilevanza del tema evidente rispetto a:

- **Vertenze di lavoro** (ad es. licenziamenti, comportamenti sul posto di lavoro, fedeltà agli obblighi, rispetto dei diritti).
- **Rapporti di famiglia** (ad es. comportamenti reciproci dei coniugi, affidamento prole, capacità economica).
- **Dispute su concorrenza e proprietà intellettuale** (ad es. atti di concorrenza sleale, violazione marchi o segni altrui o di diritti di autore, denigrazione di terzi, distrazione di clientela).

2.- Cenni sulla prova informatica.

Problema portata art. 11/2 Codice Privacy

Introduce divieto di introduz. prova illecita oppure demanda a giudice valutaz. rilevanza della stessa?

- **Per Cass. n. 18279/2010:** «gerarchia mobile» = occorre ponderata valutaz. situaz. specifica con bilanciamento interessi contrapposti'.

- **Per Trib. MI n. 9431/2016:** manca nel c.p.c. divieto di utilizzo e sanzione di nullità – scissione tra modalità di acquisizione e utilizzabilità. Quindi, valuta il giudice, mentre sogg. leso potrà agire in sede civile o penale contro acquisizione illecita.

2.- Prova informatica - esempi.

- Trib. PO n. 1100/2016: ***addebito separazione in base a condotta 'inadeguata' rivelata su Facebook.***

- Trib. RM, Sez. 1^, n. 456/2016: ***ritiene raccolta prova infedeltà coniuge da dichiarazioni postate su Facebook e confermate in giudizio da testimoni.***

- Trib. RM, n. 8432/2016: ammette telefonate registrate e SMS in quanto matrimonio determina affievolimento reciproche aspettative di riservatezza della sfera personale.

MA

- Cass. Sez. VI^, ord. n. 22677/2016: ***esclude materiale probat. raccolto illecitamente (sottrazione fraudolenta).***

2.- Prova informatica - Definizione.

Art. 2712 cc: ***«Le riproduzioni … informatiche .. le registrazioni fonografiche e … ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappre'ntate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime»***.

CAD (Dlgs. 82/2005), art. 20: *«Il documento inf'tico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 cc quando vi è apposta una firma digit., altro tipo di firma elettronica qualificata o una firma elettr. avanzata o, comunque, è formato, previa ident'zione del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore».*

Altrimenti, liberamente valutabile in giudizio.

2.- Prova informatica - Disconoscimento.

- ***Cass. Lav. n. 81507/2016:*** Mero disconoscimento non idoneo a contestare identità tra realtà 'riprodotta' e quella 'fattuale'.

- ***Cass. Lav. n. 3122/2015:*** Necessari 'elementi chiari, circostanziati, espliciti' attestanti non corrispondenza con realtà fattuale (ritiene utilizzabile DVD con filmato).

- ***Cass. Lav. n. 2117/2011:*** Contestazione generica inidonea a precludere efficacia probatoria (ammette cassetta video con registrazione condotta delle parti).

- ***Cass. Lav. n. 2912/2004:*** Non ammette pagina web su supporto cartaceo in assenza di garanzie di rispondenza e riferibilità.

2.- Prova informatica e 'incrocio' di regole

- E-mail e messaggi sogg. alle regole della corrispondenza
- Rapp. lavoro/contratto può imporre obblighi di riservatezza

Violazione = responsabilità penali o risarcitorie

- PCT (e PAT) prevedono 'specifiche tecniche' quanto a formato produzioni con problemi per file audio e video

(compressione non risolve il problema)

Soluzione ?

Forse 'masterizzazione' su CD-Rom o DVD e deposito in cancelleria (con conseguente immodificabilità) insieme a nota di spiegazione e indice contenuto (previa autorizzaz.?)

Ma

tutti i PC dei magistrati e della cancelleria dispongono di lettore e software per accesso a CD/DVD ?

3.- Studio della giurisprudenza rilevante.

3.1.- Giurisprudenza rilevante.

CEDU 28-11-2017 Antovic e Mirkovic c/ Montenegro

(Art. 8 Conv. - Diritto al rispetto della vita privata e familiare)

- 'Vita privata' termine ampio non def'bile esaustivamente e non riconducibile a 'sfera ristretta' dell'individuo.

- Include attività che si svolgono in un 'luogo pubblico' (es. posto di lavoro) o in contesto di interazione con altri.

- Aspettativa singolo alla privacy elemento importante, ma non decisive.

- Quindi aule universit. comprese nell'ambito tutelato (anche in consideraz. obblighi rapp.to lavoro docenti).

3.2.- Giurisprudenza rilevante.

CGEU Sez. 2^ 9-03-2017 CCIA Lecce c/ Manni

- Info rapp. pers. giur. rilevate per iscriz. a registri pubbl. = dati personali soggetti alle norme di trattamento

- Funzione iscriz. registri pubbl. = tutela interessi dei terzi

- Disciplina comunitaria non prevede limite temporale (con impossibilità di individuazione termine 'univoco')

- Per esigenze di certezza diritto, possibile mant'to dati oltre la cessazione della società

- Situazioni particolari (da valutare dal giud. naz. caso per caso) possono giustificare – eccezionalmente – limitazione accesso a dati registro dopo 'periodo sufficient. lungo'.

3.3.- Giurisprudenza rilevante.

Articolo di critica politica mette in dubbio esito concorso

Trib. MI 28-09-2016 n. 10374

(Ricorso ex art. 152 Codice Privacy)

Bilancia'nto tra int. fondam. (int. riservatezza – int. all'informaz.)

Divulgazione dati personali soggetta a criteri di proporzionalità, necessità, pertinenza, non eccedenza, rispetto attuale e effettiva idententità personale e morale.

Dati non aggiornati, non pertinenti, non complete e privi di interesse pubblico.

Tribunale:

- Ordina 'deindicizzazione' di URL rispetto a det. chiave ricerca,

- Condanna a spese Garante e M.d.R.

3.4.- Giurisprudenza rilevante

Si segnala anche:

- CGUE Sez. IV, 27.03.2014 (Telekabel Wien c/ Constantin Film Verleih e altri)

Afferma esigenza di bilanciamento adeguato tra diritto informazione e tutela dignità della persona.

- CGUE Grande Sez., 17.10.2017 (Bolagsupplysningen c/ Svensk Handel)

In tema di competenza giurisdizionale (è quella del luogo del centro degli interessi).

3.4.- Giurisprudenza rilevante

(segue) ***Si segnala anche:***

- CEDU Sez. IV, 6.04.2010 (Tuomela c/ Finland) 'libertà di informazione' comprende non solo notizie positive o neutrali, ma anche quelle offensive o scioccanti – personaggi in cariche o funzioni pubbliche soggetti a maggior tolleranza quanto rispetto della riservatezza – idem per terzi 'in relazione' con personaggio (entrano in sorta di 'dominio pubblico').

- CEDU Sez. Grande, 5.09.2017 (Barbulescu c/ Romania)

Licenziamento per uso private Yahoo Messenger (corr. con fratello e fidanzata). Lavorat. contesta violaz. diritto a riserv'zza.

Corte definisce concetto di 'sfera private'– compr.corrispondenza (incl. servizo di messagg'ca). Regole datore non possono azzerare rispetto riservatezza. Monitoraggio sistematico non suffi'mente evidenziato e in violaz. art. 8 Convenzione.

Grazie dell'attenzione.