Le geo - localizzanti insidie dei social network e diritto all'oblio

Avv. Monica Gobbato
Milano Università Statale

E- privacy 2012

https://twitter.com/#!/MonicaGobbato

Geolocalizzazione

Fondamentale il Parere dei Garanti Europei del
16 maggio 2011
Opinion 13/2011 WP 185

i dati relativi all'ubicazione riguardano sempre una persona fisica identificata o identificabile, ad essi si applicano le disposizioni sulla protezione dei dati personali di cui alla direttiva 95/46/CE del 24 ottobre 1995

I dati di geolocalizzazione sono una fonte potenziale di reddito
Parere 5/2005 Gruppo Garanti Europei
WP 115 adottato il 25 novembre 2005

Geolocalizzazione

Alla prima fase ne è seguita una seconda caratterizzata da servizi a valore aggiunto che non si basano più sulla localizzazione delle persone su

loro richiesta (utenti che desiderano avvalersi di un servizio) ma sul fatto di localizzarle (su richiesta di terzi).

Il valore delle info aumenta quando è collegato ad una posizione

Social Network

Rapporto e Linee-Guida in materia di privacy nei servizi di social network (*)
"Memorandum di Roma"
Adottato in occasione del 43mo incontro, 3-4 marzo 2008, Roma

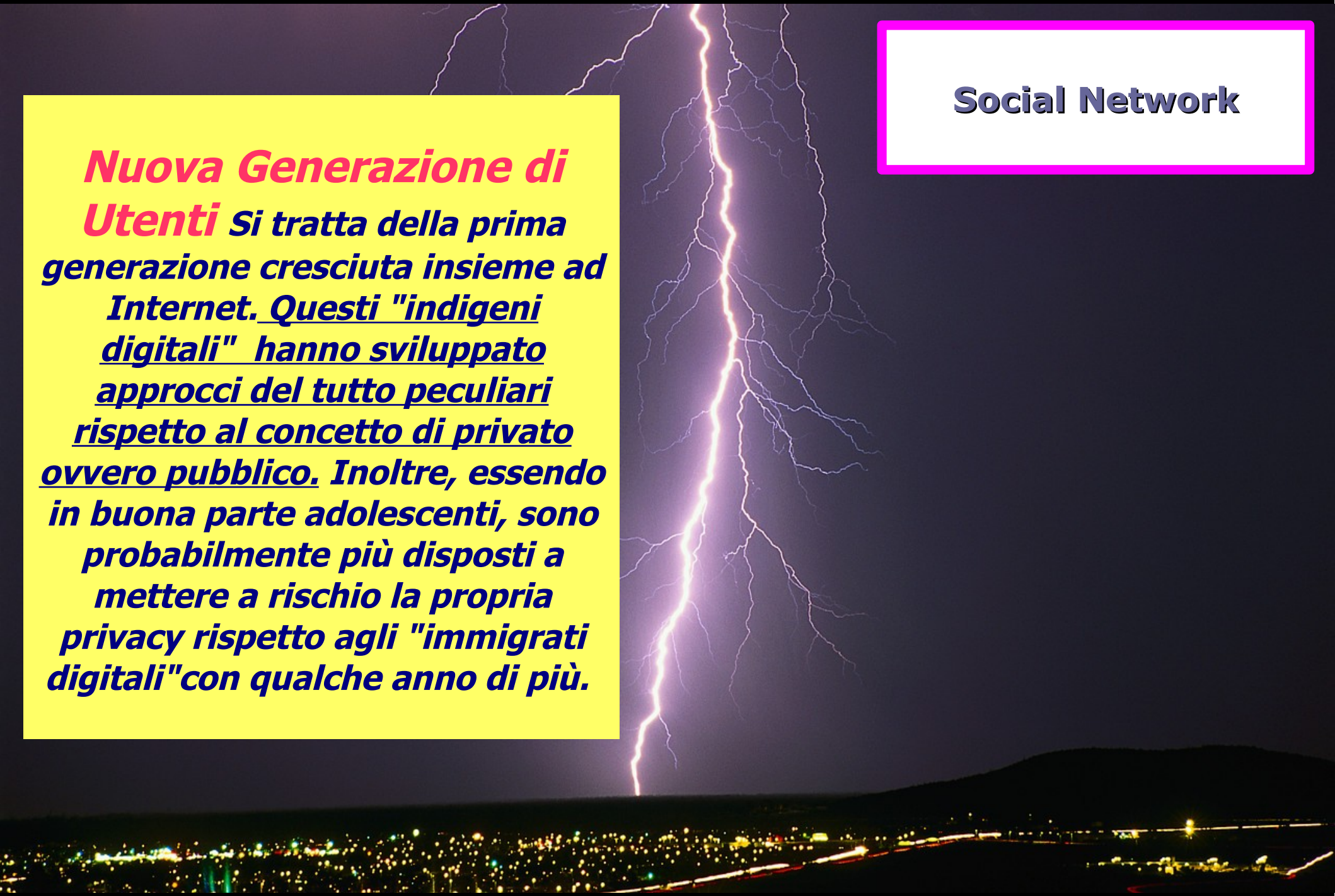
Parere 5/2009 sui social network on-line adottato il 12 giugno 2009

30ma Conferenza internazionale delle Autorità di protezione dei dati
Stasburgo, 15 - 17 ottobre 2008
Risoluzione sulla tutela della privacy nei servizi di social network

DIRETTIVA 2002/21/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 7 marzo 2002
che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro)

Geolocalizzazione

- **Art. 2, comma 1**
- c) "servizio di comunicazione elettronica", i servizi forniti di norma a pagamento consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, ma ad esclusione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti; sono inoltre esclusi i servizi della società dell'informazione di cui all'articolo 1 della direttiva 98/34/CE non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica;



Social Network

Nuova Generazione di Utenti ***Si tratta della prima generazione cresciuta insieme ad Internet. Questi "indigeni digitali" hanno sviluppato approcci del tutto peculiari rispetto al concetto di privato ovvero pubblico. Inoltre, essendo in buona parte adolescenti, sono probabilmente più disposti a mettere a rischio la propria privacy rispetto agli "immigrati digitali"con qualche anno di più.***

Geolocalizzazione

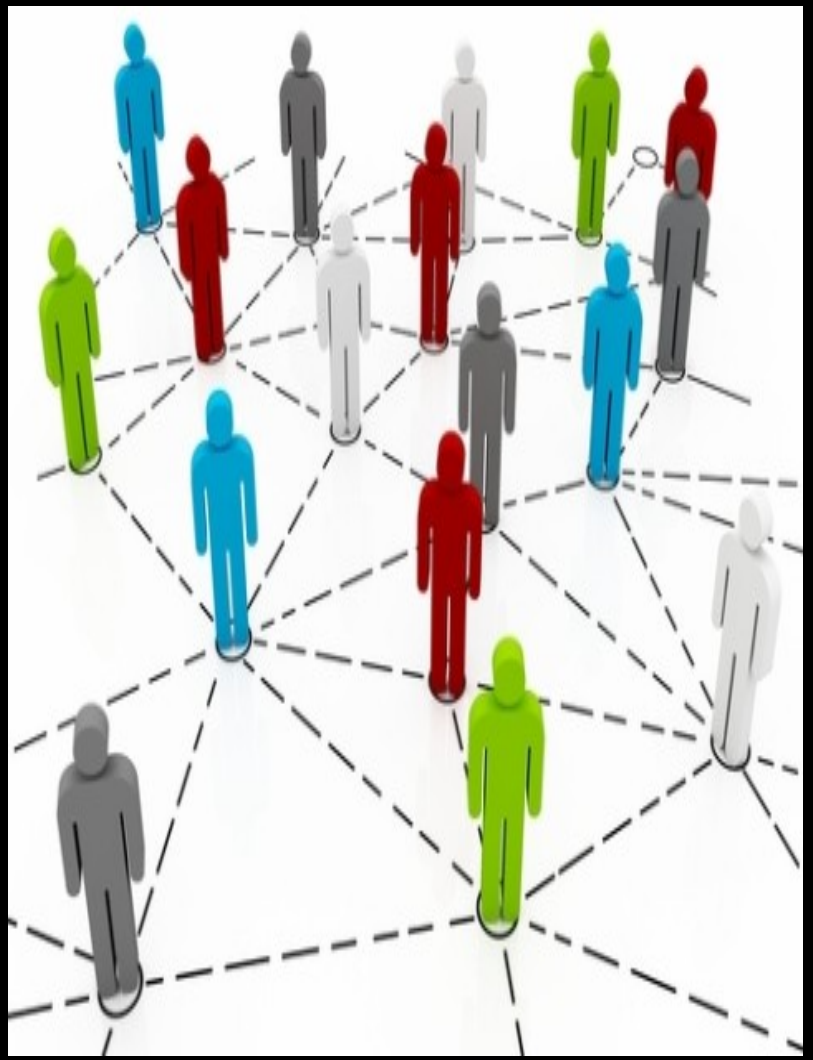
CONSAPEVOLEZZA

La tecnologia dei dispositivi mobili intelligenti consente il monitoraggio costante di dati di localizzazione.

il monitoraggio può essere fatto ***segretamente, senza informare*** l'interessato.
Il monitoraggio può essere fatto ***anche semi-segretamente, quando l'interessato si 'Dimentica'*** o non è correttamente informato del fatto che i servizi di localizzazione sono accesi su 'on', o quando le impostazioni di accessibilità dei dati relativi all'ubicazione sono cambiato da 'privati' a 'public'.

SOCIAL GRAPH

- La 'social graph' è un termine che indica la visibilità di amici in siti di social networking e la
- capacità di dedurre i tratti comportamentali dei dati riguardanti questi amici.



I rischi sinora individuati in rapporto all'utilizzo di servizi di social network sono i seguenti:

1) Niente oblio su Internet. Il concetto di oblio non esiste su Internet. I dati, una volta pubblicati, possono rimanerci letteralmente per sempre – **anche se la persona interessata li ha cancellati dal sito "originario", possono esisterne copie presso soggetti terzi.**

- ***2) L'idea ingannevole di "comunità".*** Molti fornitori affermano di trasferire le strutture comunicative dal mondo "reale" al cyberspazio. Un'affermazione frequente è che non ci sarebbero problemi, per esempio, a pubblicare dati (personali) su queste piattaforme, perché è come se si

- ***3) "Gratis" non sempre significa "a costo zero"***. realtà, molti dei servizi di social network fanno "pagare" gli utenti attraver il riutilizzo dei dati contenut nei profili personali da parte dei fornitori di servizio, ad esempio per attività (mirate di marketing.

- ***4) La raccolta di dati di traffico da parte dei fornitori di servizi di s. n.*** i quali **hanno gli strumenti tecnici per registrare ogni singolo passo dell'utente sul loro sito** .

- ***5) Utilizzo improprio dei profili utente da parte di soggetti terzi.*** **A seconda della configurazione (di default) disponibile, le informazioni contenute nel profilo (comprese immagini, che possono ritrarre sia il singolo interessato, sia altri soggetti) diventano accessibili all'intera comunità degli utenti.**

6) Rivelare più informazioni personali di quanto si creda.

Linee-guida

Alla luce delle considerazioni svolte il Gruppo di lavoro formula le seguenti raccomandazioni destinate rispettivamente **ai soggetti deputati a disciplinare i servizi di social network, ai fornitori di tali servizi ed agli utenti:**

Prevedere la possibilità di ricorrere a pseudonimi –

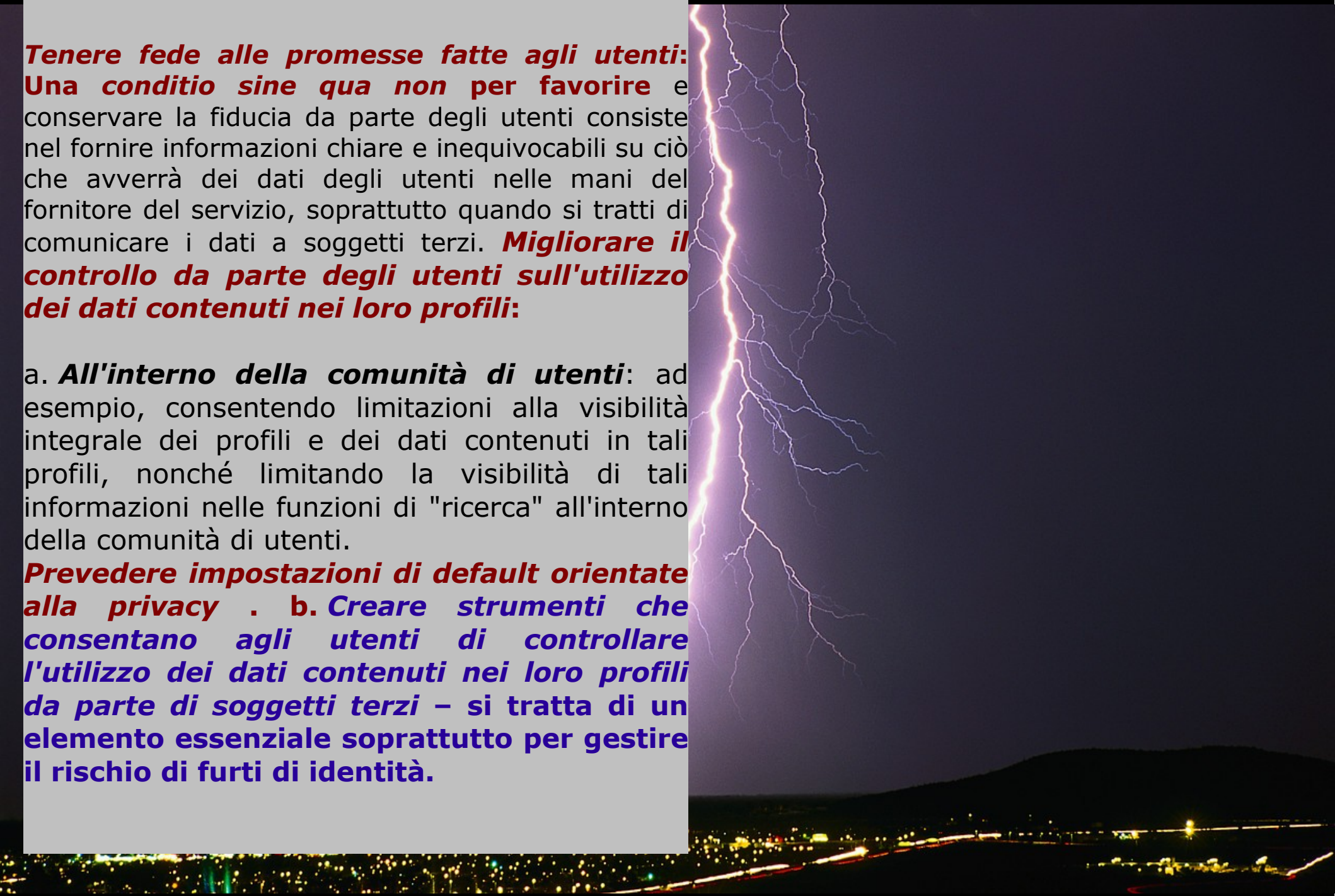
Fare in modo che i fornitori di questi servizi adottino un approccio trasparente nell'indicare le informazioni necessarie per accedere al servizio-base, in modo che gli utenti siano in grado di scegliere a ragion veduta se aderire o meno al singolo servizio, e di opporsi ad eventuali utilizzi secondari, in particolare per quanto riguarda forme (mirate) di marketing. ***Introdurre l'obbligo di notifica di eventuali violazioni dei dati relativamente ai servizi di social network*.** L'unico modo per consentire agli utenti di fare fronte, in particolare, al rischio crescente di furti di identità consiste nel notificare loro ogni violazione della sicurezza dei dati. ***Ripensare l'attuale assetto normativo con riguardo alla titolarità* dei dati personali** (in particolare relativi a soggetti terzi) pubblicati sui siti di social network, al fine eventualmente di attribuire ai fornitori di servizi di social network maggiori responsabilità rispetto alle informazioni di natura personale presenti su tali siti.

***Potenziare l'integrazione delle tematiche connesse alla privacy nel sistema educativo*.** Rivelare informazioni personali online è sempre più un fatto normale, soprattutto fra i giovani; pertanto, è necessario che i programmi didattici affrontino tematiche connesse alla privacy ed agli strumenti di autotutela disponibili. **L'informativa resa all'utente deve prendere in considerazione anche i dati relativi a soggetti terzi.** I fornitori dei servizi di social network, **dovrebbero indicare anche ciò che agli utenti è permesso o non permesso fare con i dati relativi a terzi eventualmente contenuti nei rispettivi profili** –

***Tenere fede alle promesse fatte agli utenti*: Una *conditio sine qua non* per favorire** e conservare la fiducia da parte degli utenti consiste nel fornire informazioni chiare e inequivocabili su ciò che avverrà dei dati degli utenti nelle mani del fornitore del servizio, soprattutto quando si tratti di comunicare i dati a soggetti terzi. ***Migliorare il controllo da parte degli utenti sull'utilizzo dei dati contenuti nei loro profili*:**

a. ***All'interno della comunità di utenti***: ad esempio, consentendo limitazioni alla visibilità integrale dei profili e dei dati contenuti in tali profili, nonché limitando la visibilità di tali informazioni nelle funzioni di "ricerca" all'interno della comunità di utenti.

Prevedere impostazioni di default orientate alla privacy . **b. *Creare strumenti che consentano agli utenti di controllare l'utilizzo dei dati contenuti nei loro profili da parte di soggetti terzi* – si tratta di un elemento essenziale soprattutto per gestire il rischio di furti di identità.**



APPLICABILITA'

All'interno della Comunità, il trattamento dei dati relativi all'ubicazione è subordinato al diritto nazionale dello Stato membro in cui è stabilito il responsabile del trattamento, e non a quello dello Stato Membro di cui è cittadino la persona interessata (WP 115)

Geolocalizzazione

Wp 115 DEI GARANTI EUROPEI 25 novembre 2005

Qualora il responsabile del trattamento (il fornitore del servizio a valore aggiunto) non sia stabilito in uno Stato membro, i dati relativi all'ubicazione possono essere trasferiti dall'operatore delle comunicazioni elettroniche al responsabile del trattamento solo alle condizioni (PRIVACY) CHE prevedono che la normativa in materia di protezione dei dati nel paese terzo debba garantire un livello di protezione che sia considerato adeguato dalla Commissione europea oppure che il trasferimento debba essere giustificato da altri elementi legittimanti — segnatamente, **il consenso dell'interessato, l'esistenza di un contratto concluso nell'interesse della persona cui i dati si riferiscono, un interesse pubblico superiore, la constatazione o la difesa di un diritto in sede giudiziaria o la necessità di salvaguardare gli interessi vitali della persona interessata.**

Codice Privacy Art. 17.
Trattamento che presenta rischi specifici

1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che **presenta rischi specifici** per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, **è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato**, ove prescritti.

2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

Codice Privacy
Art. 37. Notificazione del trattamento

- 1. Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:

- a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;

.... (omissis)

INFORMATIVA

- Il gruppo di lavoro ritiene che LE informazioni debbano essere fornite dal soggetto che effettua la raccolta dei dati relativi all'ubicazione per il trattamento, vale a dire dal fornitore di servizi a valore aggiunto oppure, qualora il fornitore non sia in contatto diretto con la persona interessata, dall'operatore delle comunicazioni elettroniche.

CONSENSO

- Ai sensi dell'articolo 9 della direttiva 2002/58/CE, coloro che hanno dato il proprio consenso al trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico possono ritirare il loro consenso in qualsiasi momento e devono avere la possibilità di negare, in via temporanea, mediante una funzione semplice e gratuitamente, il trattamento di tali dati.

Parere 13/2011 sui servizi di geolocalizzazione WP 185 adottato il 16 maggio 2011

- Il parere si occupa di **tre principali tipi di infrastrutture utilizzate per fornire servizi di geolocalizzazione, ovvero GPS, stazioni base GSM e WiFi**

- L'obiettivo del parere è quello di chiarire il quadro giuridico applicabile ai servizi di geolocalizzazione disponibili su e / o generati da dispositivi mobili

OBBLIGHI DERIVANTI DALLA DISCIPLINA PRIVACY

Nel contesto dei servizi di geolocalizzazione online forniti dai servizi della società dell'informazione possono essere individuate tre diverse CATEGORIE DI TITOLARI con responsabilità diverse per il trattamento dei dati personali sono

1) **TITOLARI** di una infrastruttura di geolocalizzazione;

2) Fornitore di una domanda di geolocalizzazione o un servizio specifico e

3) Sviluppatore del sistema operativo di un dispositivo intelligente mobile

1) Titolari di infrastrutture di geolocalizzazione

Simile a operatori di telecomunicazioni. Quando elaborano la posizione di un dispositivo particolare con l'aiuto delle loro stazioni radio si trovano a trattare dati personali. Dal momento che deteminano le finalità e le modalità di tali strumenti sono da considerarsi Titolari del trattamento.

2) I fornitori di applicazioni di geolocalizzazione e dei servizi

I Dispositivi mobili intelligenti consentono l'installazione di software di terzi, le cosiddette applicazioni.

Tali applicazioni possono elaborare i dati di posizione (ed altri dati) da un dispositivo mobile intelligente in modo indipendente dallo sviluppatore del sistema operativo e / o dai controllori di infrastrutture di geolocalizzazione.

Esempi di tali servizi sono: i) il meteo, ii) servizi che offrono informazioni su negozi nelle vicinanze, iii) i servizi che mostrano la posizione di amici (social network con tale funzione, Twitter, Facebook, Foursquare).

Il fornitore di un'applicazione che è in grado di elaborare i dati di geolocalizzazione è il Titolare del trattamento dei dati personali derivanti dalla installazione. Un esempio di tali servizi è l'uso di una mappa online per guidare una persona che cammina

3) Sviluppatori del sistema operativo

Lo sviluppatore del sistema operativo del dispositivo mobile può essere un Titolare per i trattamenti di geolocalizzazione quando interagisce direttamente con l'utente e raccoglie i suoi dati personali (come ad esempio richiedendo la registrazione iniziale utente e / o raccoglie informazioni sulla posizione ai fini del miglioramento dei servizi).
Lo sviluppatore deve progettare il sistema ispirandosi alla disciplina privacy per evitare il monitoraggio segreto che possa realizzarsi dal dispositivo stesso o dalle diverse applicazioni e servizi.

Responsabilità di altre parti

Ci sono molte altre parti online che permettono l'(ulteriore) trattamento della posizione
come i browser, i siti di social network o mezzi di comunicazione che consentono il 'geotagging'. Quando si incorporano dei servizi di geolocalizzazione nella propria piattaforma, si ha una responsabilità importante per decidere le impostazioni di default dell'applicazione
(Default 'ON' o 'OFF'). Tali soggetti hanno un ruolo chiave nella legittimità del trattamento per esempio quando si tratta di correttezza sulla visibilità o sulla la qualità del informazioni relativi ai dati di geolocalizzazione

Art. 11 del Codice Privacy 2° comma

I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Art. 11 del Codice Privacy

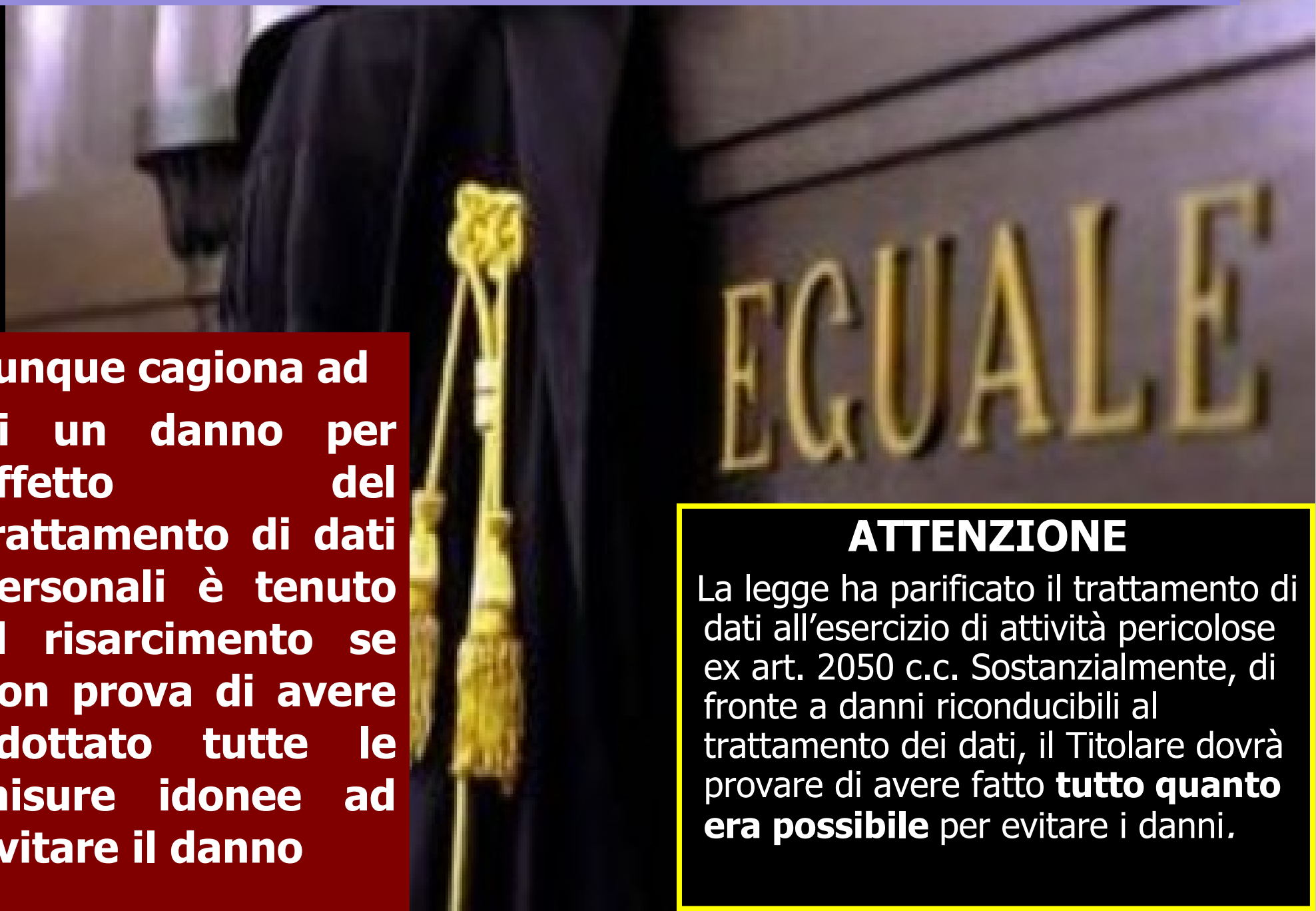
Il Titolare che continuerà a trattare i dati in violazione dei principi di cui all'art. 11 del Codice si espone alla responsabilità oggettiva di cui all’art. 2050 c.c. da attività pericolosa.

Art. 15. Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

2. **Il danno non patrimoniale** è risarcibile anche in caso di violazione dell'articolo 11.

RESPONSABILITA' CIVILE



Chiunque cagiona ad altri un danno per effetto del trattamento di dati personali è tenuto al risarcimento se non prova di avere adottato tutte le misure idonee ad evitare il danno

ATTENZIONE

La legge ha parificato il trattamento di dati all'esercizio di attività pericolose ex art. 2050 c.c. Sostanzialmente, di fronte a danni riconducibili al trattamento dei dati, il Titolare dovrà provare di avere fatto **tutto quanto era possibile** per evitare i danni.

Attività Pericolosa

E’ importante rilevare che l’art. 2050 c.c. si riferisce all'"attività pericolosa" in tutti i casi in cui vi è un’elevata potenzialità di danno, sia per la natura della attività stessa, sia per le caratteristiche dei mezzi di lavoro utilizzati.

GRAZIE

www.monicagobbato.it