REGOLAMENTO UE 679/2016

protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

Dott.ssa Elisa Palermo

I TESTI NORMATIVI VIGENTI

- Il Regolamento UE 679/2016 ha abrogato la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

- IN ITALIA: D.lgs. 30 giugno 2009, n. 196 (cd. CODICE PRIVACY) modificato dal D.lgs. 10 agosto 2018, n. 101

Il GDPR (General Data Protection Regulation)
Cosa succede?

- **1. VIENE UNIFORMATA LA DISCIPLINA A LIVELLO COMUNITARIO, ATTRAVERSO UN REGOLAMENTO**

con applicazione anche extra UE ove si trattino dati dei cittadini europei

- **2. IL GDPR DISCIPLINA UN NUOVO MONDO: I DATI DIGITALI**

quindi l'architettura normativa è totalmente diversa da quella della Direttiva precedente

Cosa succede con il GDPR?

3. **IL DIRITTO ALLA PROTEZIONE DEI DATI DIVENTA DIRITTO CIVILE EUROPEO**

4. **I DATI VENGONO PROTETTI E DISCIPLINATI IN QUANTO MATERIA PRIMA DELLA NUOVA ECONOMIA (DATA ECONOMY)**

I dati hanno un valore economico e la loro circolazione non è evitabile.

Nasce così l'esigenza di proteggere i dati e darsi regole per una circolazione sicura.

Il diritto alla protezione dei dati personali

E’ un diritto alla autodeterminazione formativa, ossia il potere di una persona fisica di verificare e controllare il trattamento di dati che lo riguardano, svolto da terzi, cui corrisponde l’obbligo del titolare di adottare misure tecniche ed organizzative di sicurezza.

DATA ECONOMY

Commissione UE COM (2017)9 final – 17 gennaio 2017

“Costruire una economia dei dati europea”

Il valore dell’economia dei dati nella UE

Anno 2014

257 mld di euro (l’1,85% del PIL della UE)

Anno 2015

272 mld di euro (pari all’1,87% del PIL della UE), per un incremento annuo del 5,6%

Anno 2020

Si stimano 643 mld di euro, pari al 3,17% del PIL della UE

Le informazioni personali come nuova moneta virtuale (DATA ECONOMY)

Tutto ciò che viene pubblicato, scritto o postato, come anche i video o le foto, è destinato a rimanere a disposizione di chiunque.

Attualmente la tecnologia non è in grado di garantire il rispetto delle norme poste a tutela della privacy dei singoli.

Le informazioni fornite vengono vendute o scambiate con aziende operanti nell'e-commerce o con spammer.

Il rischio è quello di perdere il controllo dell'utilizzo dei propri dati una volta pubblicati in rete, in particolare nei social, con l'aggravante che, la permanenza in rete delle informazioni ponga significativi problemi anche in merito al diritto all'oblio.

DATA ECONOMY – La logica economica, niente è gratis

Le Aziende che gestiscono Social Network solitamente si finanziano vendendo pubblicità mirate.

Il valore di queste imprese è strettamente legato alla loro capacità di analizzare in dettaglio il profilo degli utenti, le abitudini e i loro hobby, ma anche le condizioni di salute e l'orientamento politico e sessuale e le reti di contatti (***profilazione***) anche semplicemente attraverso la gestione dei *"like"* da te apposti ad articoli o contenuti in rete. Poi rivendono le informazioni ad altre imprese che si occupano di fare offerte commerciali specifiche o di sostenere campagne di vario genere.

DATA ECONOMY – La logica economica, niente è gratis

Le informazioni raccolte sugli utenti sono infatti utilizzate per monitorare e prevedere gli acquisti, le scelte e i comportamenti degli utenti.

Dunque dietro l'offerta di un servizio "gratuito" reso dal web, si nasconde in realtà lo sfruttameto economico dei dati degli utenti (***data economy***).

I DIRITTI DEGLI INTERESSATI – CAPO III GDPR

- diritto all'informativa (ARTT. 12-14)
- diritto all'accesso (ART. 15)
- diritto di rettifica (ART. 16)
- diritto alla cancellazione (all'oblio) (ART. 17)
- diritto alla limitazione del trattamento (ART. 18)
- diritto alla portabilità (ART. 20)
- diritto all'opposizione (ART. 21)

Diritto all'informativa (ARTT. 12-14)

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Diritto all’accesso (ART. 15)

1. *L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:*

a) *le finalità del trattamento;*

b) *le categorie di dati personali in questione;*

c) *i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati…..*

d) *il periodo di conservazione dei dati personali previsto….*

e) *l'esistenza del diritto di chiedere al titolare la rettifica o la cancellazione dei dati personali o la limitazione del trattamento o di opporsi al loro trattamento;*

f) *il diritto di proporre reclamo a un'autorità di controllo;*

g) *qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;*

h) *l'esistenza di un processo decisionale automatizzato, compresa la profilazione…*

Diritto di rettifica (ART. 16)

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Diritto all’oblio (ART. 17)

In determinate circostanze *“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…”*

Il diritto all'oblio

Si tratta di una creazione della giurisprudenza che, con la sentenza della **Cassazione (numero 3679 del 9 aprile 1998),** ha affermato che "Il diritto di cronaca può poi risultare limitato dall'esigenza dell'attualità della notizia, quale manifestazione del diritto alla riservatezza, intesa quale giusto interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata, salvo che per eventi sopravvenuti il fatto precedente ritorni di attualità e rinasca un nuovo interesse pubblico all'informazione".

Diritto all’Oblio - la Sentenza n. 5525/2014 della terza sezione civile della Cassazione

La Sentenza ha imposto l'aggiornamento delle vecchie notizie, rafforzando il diritto all'oblio al tempo del web (come nel caso di specie) inserendo un obbligo da parte delle aziende editoriali. In sostanza, se una notizia è conservata nell'archivio storico della testata ed è disponibile grazie ai motori di ricerca, il titolare dell'organo di informazione deve curarne l'aggiornamento. E a nulla vale, in questo caso, opporre il fatto che nel mare magnum di internet è possibile comunque reperire ulteriori notizie sull'argomento specifico.

Diritto all’Oblio - la Corte Europea dei Diritti dell'Uomo

In tema di diritto all'oblio, inoltre, ha dato una significativa risposta con la sentenza "Google" del 13 maggio 2014, causa C-131/12. Il colosso di Mountain View è stato condannato a rimuovere i link dopo alcuni anni in ragione del diritto all'oblio e la stessa situazione dovrebbe realizzarsi per gli archivi di tanti giornali online.

Diritto alla limitazione del trattamento (ART. 18)

In alcuni casi *“l'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento…”*

Diritto alla portabilità (ART. 20)

“L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso o su un

b) Il trattamento sia effettuato con mezzi automatizzati.

Diritto all’opposizione (ART. 21)

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano (…) compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

DATA BREACH – ART. 33

- *“In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza…”*
- *“Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.”*

DATA BREACH – ART. 34

“Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.”

DATA BREACH

Si profila un DATA BREACH ogni volta che avviene la distruzione, perdita, modifica, divulgazione non autorizzata o accesso a dati personali trasmessi, conservati o trattati a seguito di:

- **Accesso abusivo ai sistemi**
- **Sottrazione fraudolenta di dati**
- **Perdita accidentale di dati**

Comunicazione al Garante: entro 72 ore

Comunicazione all'interessato: tempestiva

NUOVE DEFINIZIONI DEL GDPR

- **Dati personali (art. 4 lett. 1):** dati che rendono identificato o identificabile un soggetto
- **Dati particolari:** più tutelati (ex dati sensibili)
- **Dato Pseudomizzato:** dato in cui l'identificatore viene sostituito da indicatori fittizi o pseudonimi
- **Dato de-identificato (art. 11):** dati a cui sono stati rimossi gli identificatori diretti o indiretti, con rischio residuo di re-identificazione.

NUOVE DEFINIZIONI DEL GDPR

- **Dato anonimo:** è il dato non identificabile o re-identificabile. Esce così dalla sfera di applicazione del Regolamento, (es. quelli acquistati da altri che si vincolano contrattualmente a non cedere mai l'identificatore utile a re-identificare il dato: nelle mani del cedente saranno dati pseudonomizzati, nelle mani del cessionario saranno dati anonimi)**.**
- **Profilazione** (trattamento automatizzato di dati personali per analizzare)

Trattamento di categorie particolari di dati personali – Art. 9 GDPR

Il regolamento introduce il nuovo concetto di DATI PARTICOLARI, che sostituisce i precedenti DATI SENSIBILI, aggiungendo di fatto al vecchio impianto:

- I dati biometrici, quelli atti ad identificare in modo univoco una persona fisica
- I dati atti a rilevare l'orientamento sessuale di una persona.

Art. 9 GDPR, comma 1

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Art. 9 GDPR, comma 2

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

a. *Consenso Informato.*
b. *Necessità per diritti del Titolare in materia di diritto del lavoro e della sicurezza e protezione sociale.*
c. *Per tutela di un interesse vitale dell'interessato, in stato di incapacità fisica o giuridica a prestare consenso.*
d. *Se trattati da Ass.ni o Fond.ni senza scopo di lucro, senza divulgazione esterna.*
e. *Se è l'interessato ad avere reso pubblici i propri dati.*
f. *Diritto di difesa in sede giurisdizionale.*
g. *Interesse pubblico, purchè il trattamento sia proporzionato.*
h. *Medicina preventiva – lavoro – idoneità fisica al lavoro, diagnosi, assistenza o terapia sanitaria. IN QUESTI CASI NON SERVE CONSENSO – NON C'è OBLIO*
i. *Interesse pubblico in sanità pubblica, minacc epe rla salute a carattere transfrontaliero. NO OBLIO*
j. *Archiviazione di pubblico interesse, ricerca scientifica, storica – fini statistici*

SOCIAL PRIVACY – Come tutelarsi nell'era dei Social Network

Il mondo delle reti social è in continua evoluzione e il Garante della Privacy nazionale cerca di tutelare con efficacia le persone fisiche che ne fanno uso, già da prima della entrata in vigore del GDPR Europeo.

I social network offrono indubbiamente vantaggi in termini di comunicazione e scambi documentali .

Tuttavia i rischi legati ad un utilizzo improprio o fraudolento dei dati trasmessi, si moltiplicano esponendo gli utenti a danni alla reputazione, furti di identità e veri e propri abusi al diritto di privacy.

SOCIAL PRIVACY – Come tutelarsi nell'era dei Social Network

Non esistono più barriere tra la vita digitale e quella reale e ciò che succede online impatta anche fuori da Internet .

I S.N. possono dare l'idea di uno spazio personale con il nostro interlocutore e questo errato senso di intimità può spingere gli utenti ad esporre troppo la propria vita privata e professionale e a rivelare informazioni confidenziali, orientamenti politico, scelte sessuali, fede religiosa, condizioni di salute provocando gravi "effetti collaterali" anche a distanza di anni, che non vanno sottovalutati.

SOCIAL PRIVACY – Come tutelarsi nell'era dei Social Network

Anche l'idea di impunità, trasmessa dalla possibilità di utilizzare messaggi che si "autodistruggono" (snap-chat) o di nascondersi dietro forme di anonimato, può favorire in rete atteggiamenti aggressivi o violenti, verso soprattutto le fasce più deboli.

Il Mito dell'Anonimato

Coloro che pubblicano testi, immagini, video allo scopo di danneggiare l'immagine o la reputazione di altre persone, sono perseguibili per legge.

Infatti l'anonimato in rete non è ammesso per commettere reati e le autorità competenti dispongono di strumenti per intervenire e scoprire il colpevole.

Il consenso…

Quando metti online una foto di un tuo amico o di un familiare o lo “tagghi”, domandati se stai violando la sa privacy.

Nel dubbio chiedigli il consenso..

SOCIAL PRIVACY – Come tutelarsi nell'era dei Social Network

La dignità della persona e il diritto alla riservatezza non perdono la loro efficacia su Internet.

L'Autorità Italiana per la Protezione dei dati Personali (Garante Privacy) interviene a garanzia di quanto dettato nella normativa Europea per il territorio di propria competenza.

SOCIAL PRIVACY – Come tutelarsi nell'era dei Social Network

Il Web è spesso visto come un luogo senza regole, dove ogni utente può dire o fare quello che vuole.

In realtà le regole di civile convivenza e le norme a tutela della riservatezza, diffamazione, violazione della dignità personale valgono nella vita reale così come online.

Non esistono zone franche dal buon senso e dalla applicazione delle norme.

SOCIAL PRIVACY – Come tutelarsi nell'era dei Social Network

Quando i dati personali vengono inseriti in un Social N. ne perdi il controllo.

Possono essere registrati da tutti i tuoi contatti e dai componenti dei gruppi cui si è aderito, rielaborati, diffusi anche a distanza di anni.

A volte, accettando di entrare in un Social Network, concedi al fornitore del servizio la **licenza di usare senza limiti temporali** il materiale che inserisci online (foto, opinioni, chat, ecc.).

I falsi profili e l’autodistruzione dei messaggi

Attenzione ai falsi profili. Bastano la foto, il tuo nome e qualche informazione sulla tua vita, per impadronirsi online della tua identità.

Molti utenti pensano che l’invio di messaggi che si autodistruggono (snap-chat) possa tutelarli dal rischio di un uso inappropriato del materiale condiviso. Questo può spingere ad esempio a scambiare messaggi dal contenuto sessualmente esplicito senza farsi troppi problemi (sexting). Tutto quello che è condiviso però può sempre essere salvato e riutilizzato.

Attenzione.

Disattivazione o cancellazione?

Se decidi di uscire da un Social Network a cui sei iscritto ti è permesso solo di disattivare il tuo profilo e non di cancellarlo.

E così i dati, i materiali che hai messo online, potrebbero essere comunque conservati nei server e negli archi informatici della Azienda.

Leggi bene le condizioni di utilizzo e le garanzie privacy che accetti al momento dell'iscrizione.

La sede di applicazione della legge

La maggior parte dei Social Network ha sede all'estero, e così i loro server ed archivi informatici.

In caso di problemi insorti per violazione di privacy, non sempre è garantita la tutela di leggi italiane ed europee.

Le società che offrono servizi da sedi dislocate in Paesi della UE devono sempre rispettare la normativa comunitaria e in essi è presente una Autorità di Protezione dei Dati (Data Protection Authority) che interverrà a tutela delle violazioni della Privacy.

Occhio ai cavilli…

E’ importante Informarsi su chi gestisce il Social Network e quali garanzie offre rispetto al trattamento dei dati personali.

E’ proprio diritto sapere come vengono utilizzati i dati resi disponibili nelle sezioni “privacy policy”.

E’ importante accertarsi di poter recedere dal servizio, cancellare, trasferire i dati inseriti e relativi alla tua identità. Leggere sempre bene il contratto e le condizioni d’uso e le modifiche unilaterali introdotte dal fornitore del servizio, che spesso cambiano i livelli di privacy opzionati dal’utente.

Il caso: lo scandalo Facebook-Cambridge Analytica

Lo **scandalo dei dati Facebook-Cambridge Analytica** è stato uno dei maggiori scandali politici avvenuti all'inizio del 2018, quando fu rivelato che Cambridge Analytica aveva raccolto i dati personali di milioni di account Facebook senza il loro consenso e li aveva usati per scopi di propaganda politica. È stato definito come un momento di spartiacque nella comprensione pubblica dei dati personali e ha provocato un forte calo del prezzo delle azioni di Facebook, alla quale si è chiesta una regolamentazione più rigorosa sull'uso dei dati personali da parte delle aziende tecnologiche.

L'evento fu significativo in quanto accese i riflettori sugli standard etici dei social media.

I sostenitori dei consumatori hanno chiesto una maggiore protezione degli utenti online e in materia di diritto alla privacy, oltre a limitare la disinformazione e la propaganda.

Il caso: lo scandalo Facebook-Cambridge Analytica

Il CEO (Amministratore Delegato) di Facebook si è dapprima scusato per la situazione con Cambridge Analytica sulla CNN, definendolo come "un problema", "un errore" e una "mancanza di fiducia“.

A seguito di un’iniziale riluttanza nel definire la questione come una "violazione dei dati“, Facebook si è poi impegnata a modificare e riformare la privacy policy del Social Network, al fine di prevenire eventi simili in futuro.

Ad aprile 2018 si è deciso di implementare il Regolamento generale Per La Protezione Dei Dati (GDPR) in tutte le aree e non più soltanto nella zona europea.

Amazon sostiene di aver sospeso l'utilizzo del loro Amazon Web Services nei confronti di Cambridge Analytica nel momento in cui è stato reso noto che il loro servizio stava raccogliendo informazioni personali.

La banca italiana UniCredit ha smesso di pubblicizzarsi e fare marketing su Facebook.

Ad inizio luglio 2018, la commissione del Regno Unito ha annunciato di essere intenzionata a multare Facebook per una somma pari a £ 500,000 (€546.173) a causa dello scandalo, la cifra massima consentita all'epoca della violazione, sostenendo che Facebook "ha contravvenuto la legge non salvaguardando le informazioni dei propri utenti."

Nel luglio 2019, la Federal Trade Commission ha stabilito di multare Facebook per una cifra pari a $5 miliardi di dollari (€4 miliardi e mezzo circa) per sistemare la situazione riguardante lo scandalo.

Più social privacy e meno App e Spam

E’ buona abitudine controllare spesso i **livelli di privacy del proprio profilo**, per verificare da chi essere contattati, chi può leggere quello che posti, chi può commentare i tuoi post, che diritti hanno gli utenti appartenenti ai gruppi a cui ci si iscrive.

E’ bene limitare al massimo la **disponibilità di informazioni** (geolocalizzazione, reperibilità dei dati nei motori di ricerca ecc.).

Controllare sempre quali **diritti di accesso** si concedono alle **App** installate su smatphone o tablet, affinchè non possano utilizzare i tuoi dati personali (rubrica, foto, telefonate..).

Se non desideri ricevere **pubblicità** ricordati che puoi rifiutare il consenso all’utilizzo dei dati per attività mirate di pubblicità, marketing e promozioni.

Le regole post GDPR: usi vietati e leciti dei nostri dati – I dati personali resi pubblici

I dati personali possono essere resi pubblici dall'interessato e tale circostanza ne autorizza di per sé il trattamento, anche in caso di **dato personale cosiddetto particolare** (che rivela ai sensi dell'art. 9 **GDPR** l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, biometrici, dati relativi alla salute, alla vita oppure orientamento sessuale).

Il trattamento dei dati personali resi accessibili acquista particolare rilievo rispetto al tema delle pubblicazioni su social network, quali piattaforme telematiche sulle quali il dato non solo circola ma può essere anche estratto, diffuso, raffrontato per altro trattamento con finalità diverse ed ulteriori, quale il marketing.

Il dato personale si considera **reso pubblico** quando esso è conoscibile da chiunque perché contenuto in registri, elenchi, atti o documenti pubblici o, altrimenti, perché **reso noto** direttamente dall'interessato, anche attraverso il proprio comportamento in pubblico.

Nella **prima ipotesi** sarà la mera presenza del dato nel documento con valenza pubblica a renderlo conoscibile a chiunque, mentre nella **seconda ipotesi** la notorietà deriverà da un comportamento dell'interessato che appunto decide di **condividere l'informazione che lo riguarda** (ad esempio con un post caricato sul proprio profilo Facebook).

Ne deriva che la valenza pubblica del dato può scaturire dal trattamento che ne viene fatto (inserimento e consultazione di documento pubblico per legge) o, viceversa, consistere nella scelta dell'interessato di condividere l'informazione (caricamento della foto sul social-network).

Le regole post GDPR: usi vietati e leciti dei nostri dati – La base giuridica del trattamento

Il trattamento dei dati personali resi manifestatamente pubblici dall'interessato non sfugge al principio di liceità del trattamento ex art. 6 GDPR e, più specificatamente:

- nell'ipotesi di dati personali pubblici "funzionali" la base giuridica del trattamento potrà rinvenirsi nell'adempimento di un obbligo legale cui è soggetto il Titolare del trattamento ai sensi dell'art. 6, par. 1, lett. c (si pensi agli albi professionali);
- nell'ipotesi di dati personali pubblici "non funzionali" il trattamento può avvenire all'inizio se necessario all'esecuzione del contratto di servizio ai sensi dell'art. par. 1, lett. b, (per esempio quando ci si iscrive al social-network) e, successivamente, per consenso espresso o comportamento dell'interessato (per esempio ogni post o foto inseriti sul social network) rispetto alla finalità.

Le regole post GDPR: usi vietati e leciti dei nostri dati – La base giuridica del trattamento

Deve evidenziarsi infatti che anche laddove l'art. 9, par. 2, lett. E del GDPR rende lecito il trattamento di dati personali particolari se resi pubblici dall'interessato, la base giuridica del trattamento è, indirettamente, proprio il consenso che l'interessato esercita con atto concludente quando rende noto il proprio dato personale. In tal senso l'art. 4, n.11, identifica il consenso come *qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato con la quale manifesta il proprio assenso mediante dichiarazione o* ***azione positiva inequivocabile****.*

Ne consegue che richiedere di **condividere dati su un social network costituisce indubbio consenso a rendere pubblicamente accessibili quelle informazioni, ovviamente nei limiti delle finalità cui il trattamento è teso.**

Ecco che, sotto tale ultimo aspetto, l'informativa che il Titolare del trattamento deve rendere ai sensi dell'art. 13 GDPR non costituisce solo un diritto astratto dell'interessato ma piuttosto **uno strumento essenziale di formazione del consenso informato e libero** ed il confine della liceità del trattamento rispetto alle finalità che vi devono essere specificate.

Le regole post GDPR: usi vietati e leciti dei nostri dati – Il limite della finalità di trattamento

Il trattamento dei dati personali resi manifestamente pubblici è strettamente connesso al principio di limitazione delle finalità del loro trattamento di cui all'art. 5, par. 1, lett b, GDPR, poiché soprattutto il consenso (dichiarato o attuato) al trattamento del dato personale accessibile può riferirsi solo agli scopi determinati, espliciti, legittimi e compatibili la sua pubblicizzazione (per esempio la finalità di interazione e contatto fra utenti di social-network).

In altri termini, **il consenso al trattamento di propri dati personali tramite inserimento ed interazione su piattaforme telematiche di contatto deve intendersi inerente alle funzioni tipiche del social network** e non anche a finalità ulteriori, quali spam e marketing.

Un caso di riferimento è, infatti, quello deciso già prima del GDPR dal **Garante per la protezione dei dati personali** il 21.09.2017 (doc. web 7221917) in tema di email promozionali con il quale veniva dichiarato illecito il trattamento di dati personali (indirizzi di posta elettronica) acquisiti tramite Linkedin e Facebook e, in assenza di specifico consenso, utilizzati per l'invio di numerose comunicazioni promozionali. **In tale pronuncia l'Autorità ribadisce, infatti, che la disponibilità online dei dati non legittima il trattamento per qualsiasi finalità** (quali quelle promozionali) ulteriori a quelle sottese alla loro pubblicazione

Le regole post GDPR: usi vietati e leciti dei nostri dati – Il limite della finalità di trattamento

A seguito dell'entrata in vigore del GDPR e della modifica del Codice Privacy dal D. Lgs. n.101/2018, è previsto oggi che il trattamento di dati accessibili per finalità di promozione commerciale deve presupporre il consenso specifico dell'interessato.

Il nuovo **art. 129 del Codice Privacy** impone infatti che i dati personali presenti in elenchi cartacei o elettronici a disposizione del pubblico devono essere oggetto di consenso espresso e specifico dell'interessato al loro trattamento per scopi pubblicitari o commerciali se ulteriori rispetto e quello tipico cui è volto l'elenco.

Ulteriormente il successivo **art. 130 del Codice Privacy** indica la regola generale per cui "*l'uso di sistemi automatizzati di chiamata o di comunicazione di chiamata, senza l'intervento di operatore, per scopi di pubblicità, vendita o ricerche di mercato e comunicazione commerciale è lecito con il consenso del contraente o utente*", con estensione della citata condizione di liceità anche alle comunicazioni mediante posta elettronica, telefax, MMS ed SMS o di altro tipo.

Le regole post GDPR: usi vietati e leciti dei nostri dati – Il principio di minimizzazione

Collegato al principio della finalità del trattamento è infine quello di minimizzazione di cui **all'art. 5, par. 1, lett. c, GDPR** a tenore del quale "*i dati sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*".

Ne consegue che lo scopo determina la liceità del trattamento non solo dall'esterno (riguardo a finalità distinte ed ulteriori) ma anche al suo interno, potendo far riferimento solo a quelle informazioni minime effettivamente necessarie al suo raggiungimento.

Le regole post GDPR: usi vietati e leciti dei nostri dati – Le finalità giornalistiche e di informazione

Caso particolare del trattamento dei dati resi accessibili, anche tramite comportamenti dell'interessato o per le sue qualità soggettive (si pensi a persone di rilevanza pubblica), va rilevato che esso può avvenire per finalità giornalistiche e di informazione disciplinate **dall'art. 137 del nuovo Codice Privacy**.

Tale trattamento è lecito anche senza consenso (anche per i dati particolari e giudiziari ex artt. 9 e 10 GDPR) purché attuato da esercenti la professione giornalistica, per il perseguimento delle relative finalità e nel rispetto delle Regole deontologiche (provvedimento del Garante del 29.11.2018, pubblicate in GU il 4.01.2019, n.3, doc. web n. 9067692), nei limiti del diritto di cronaca, dell'essenzialità dell'informazione ed in bilanciamento con la tutela dei diritti e libertà delle persone fisiche (art. 1, par. 2, GDPR) con particolare riferimento all'essenzialità dell'informazione rispetto all'interesse pubblico.

Le regole post GDPR: usi vietati e leciti dei nostri dati – Conclusioni

Il trattamento dei dati personali sia comuni sia particolari ai sensi dell'art. 9, par. 1, lettera e, GDPR resi manifestatamente pubblici dall'interessato anche tramite social network deve intendersi legittimo se fondato su una delle condizioni di liceità dell'art. 6 GDPR, fra le quali deve attribuirsi particolare rilievo al consenso dell'interessato.

Ne consegue che l'accessibilità del dato costituisce solo una sua caratteristica ma mai il presupposto giuridico che ne autorizzi qualunque trattamento.

Le regole post GDPR: usi vietati e leciti dei nostri dati – Conclusioni

La condizione di liceità sarà ulteriormente limitata dai **principi generali definiti all'art. 5 del GDPR**

1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali **(«limitazione della finalità»);**

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («**limitazione della conservazione**»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («i**ntegrità e riservatezza**»).

Il diritto alla privacy nel bambino

I bambini, in quanto minori, hanno bisogno della certezza che i loro genitori e gli adulti in generale si occupino e proteggano la loro privacy e si facciano quindi “garanti” dei loro diritti.

Invece non sempre le insidie che può nascondere il web sono note a chi vi naviga.

Il fenomeno dello “sharenting”

Recenti statistiche testimoniano come, nonostante le tecnologie *touchscreen* siano proprietà dell’adulto, in realtà anche i bambini entrino in contatto con esse, già prima del compimento di tre anni di età.

Oltre al ruolo di “utente” dei social network, il bambino assume spesso anche quello di “contenuto” di immagini, video o post pubblicati da parte dei loro genitori che desiderano raccontare e mettere in luce le proprie esperienze vissute con i figli e condividerle con amici e conoscenti.

Questo fenomeno viene definito “sharenting”, neologismo che deriva dalla fusione delle parole ***share (condividere)*** e ***parenting (genitorialità)*** e mette in luce la tendenza dell’essere umano alla “vetrinizzazione”.

Lo sharenting

Quando un bambino appare in rete, circa nel 45% dei casi viene riportato anche il suo nome di battesimo.

Queste tracce digitali su cui i bambini non hanno controllo vanno a sedimentarsi in rete diventando parte della loro **identità digitale**.

I Social Network vengono spesso visti come dei "palcoscenici virtuali" che gratificano il genitore dandogli la possibilità di condividere preoccupazioni, dubbi, domande sulla gestione dei figli, soprattutto nella fascia di età 0-3 anni, fornendo loro sensazioni rassicuranti.

Rischi della pubblicazione di immagini dei bambini

Il pericolo maggiormente percepito dall'opinione pubblica è legato al fatto che le foto dei minori inserite in rete, in particolare nei Social Network, possano diffondersi tra sconosciuti, essere scaricate, modificate e condivise su siti utilizzati da pedofili.

Rischi della pubblicazione di immagini dei bambini

- La possibilità che delinquenti utilizzino i volti ricavati dalle fotografie per realizzare **fotomontaggi** e esporre le foto ritoccate su **siti di pedofili**.
- Il **rapimento** può essere un altro grande pericolo, se l'adulto non presta troppa attenzione alle impostazioni della privacy nei social, e fa sapere anche a sconosciuti dove si trova il bambino.
- Altra insidia legata alla pubblicazione online può essere il "**rapimento digitale**", ossia il **furto dell'identità online**, che consiste nella manipolazione di foto di bambini trovate on-line facendo credere che siano figli propri.

Ancora il "**child-grooming**" in cui il cyberpredatore raccoglie informazioni sul bambino e sulla sua famiglia instaurando una connessione virtuale volta a scopi illeciti.

Rischi della pubblicazione di immagini dei bambini

- Accanto a comportamenti con rilevanza penale potrebbero portare i bambini a diventare future vittime di **cyberbullismo**.

“Tutto ciò che noi postiamo rimane online, perciò oltre che nuocere alla vita dei bambini lo sharing senza criteri potrebbe contribuire a creare una sorta di dossier digitale sui piccoli”

*(**Giuseppe Riva**)*

Ma cosa dice la legge?

La **Convenzione ONU sui diritti dell'infanzia e dell'adolescenza**, approvata dall'Assemblea Generale delle Nazioni Unite il 20 novembre 1989, contiene principi fondamentali fra cui il ***diritto del minore ad essere ascoltato***. Con questa Convenzione il bambino passa da una condizione di inferiorità rispetto ai genitori a persona con libertà e diritti, posta sotto la responsabilità dell'adulto che deve impegnarsi a rispondere ai suoi diritti e bisogni.

Carta dei diritti fondamentali dell'Unione Europea

Stilata a Nizza nel 2000, acquisì efficacia diretta solol'1/12/**2009**, con l'adozione del **Trattato di Lisbona**. Quest'ultima, cita **all'art. 24** quali sono i **diritti del bambino**:

"I bambini hanno diritto alla protezione e alle cure necessarie per il loro benessere. Essi possono esprimere liberamente la propria opinione; questa viene presa in considerazione sulle questioni che li riguardano in funzione della loro età e della loro maturità. In tutti gli atti relativi ai bambini, siano essi compiuti da autorità pubbliche o da istituzioni private, l'interesse superiore del bambino deve essere considerato preminente…".

La pubblicazione

Per “pubblicazione” si intende la divulgazione di un’immagine attraverso un qualsiasi mezzo che la renda pubblica: mostre, siti internet, riviste, cartelloni pubblicitari, ecc.

Vi è una netta differenza tra il caso di pubblicazione della foto del minore **per scopi privati** (inserendo tutti i sistemi di sicurezza possibili) e **per scopi pubblicitari**: infatti in questo secondo caso, è necessario far firmare una liberatoria ai genitori e sottoporre agli stessi l’informativa sulla privacy.

La pubblicazione di immagini di minori

Ai genitori è consentito pubblicare foto o video riguardanti i propri figli (non esiste alcun divieto che sostenga il contrario), l'importante è che lo facciano con consapevolezza e senza metterlo in ridicolo, e che entrambi i coniugi siano d'accordo con questa scelta (art. 10 Codice Civile).

Nel 2017 il tribunale di Mantova ha pubblicato una sentenza sulla condivisione di immagini che riguardano i minori, stabilendo che per quanto riguarda le foto dei figli occorre il consenso di entrambi i genitori.

Cosa dice il Garante della Privacy ?

Nel dicembre 2016 ha formalizzato il **criterio della prudenza nella pubblicazione di foto o video nel Web**

Dichiarando necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video.

Questo consenso, per quanto riguarda l'infanzia, è in mano a chi esercita la patria potestà sul minore.

Reg. UE 2016/679 (GDPR)

“I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali”.

Come prevenire i rischi

La polizia postale sconsiglia ai genitori la diffusione di foto dei propri figli a causa della diffusione online di nuove modalità di adescamento dei minori nel cosiddetto darknet.

La documentazione come forma di trasmissione di esperienze La fotografia come vera e propria azione educativa

Nei servizi per l'infanzia è ritenuta utile la **documentazione di un progetto educativo**, come i video e le fotografie.

Tale documentazione si costruisce attraverso. l'**osservazione** di una situazione, l'analisi e la selezione dei materiali osservativi e successivamente attraverso la **rielaborazione**, la traduzione e l'interpretazione di questi ultimi

La fotografia può essere utile sia nello scambio di idee, messaggi o informazioni tra educatori e famiglie, sia per far riflettere i piccoli sul lavoro svolto annualmente e permette di rivedere ciò che è stato osservato, acquisendo più informazioni e dettagli, che a occhio nudo potrebbero essere sfuggiti.

La privacy nei servizi per l'infanzia

- Nei servizi per l'infanzia c'è una privacy da salvaguardare. Spesso gli asili "postano" sui Social Network gli scatti fatti ai piccoli durante le attività didattiche quotidiane, o durante le gite scolastiche.

- Tale trattamento dei dati deve essere previamente autorizzato dai genitori. Il servizio deve acquisire un **preventivo consenso alla pubblicazione su siti istituzionali o sui social della scuola**, delle foto scattate in occasione di eventi (come ad esempio le recite) raffiguranti i minori, in particolare quelle dove sono riconoscibili i volti.

- Il rischio infatti è quello di commettere un **reato**, con conseguente obbligo di risarcimento del danno.

La privacy nei servizi per l'infanzia

In qualità di pubblica amministrazione, la scuola tratta i dati degli studenti in forza di legge o di regolamento e pertanto **non è tenuta a chiedere il consenso** per la pubblicazione delle fotografie che ritraggono studenti, se rispetta le finalità istituzionali e didattiche proprie della scuola.

L'istituzione deve però dimostrare che la pubblicazione di fotografie o video è indispensabile per la valenza di uno o più progetti didattici. Per fare questo è necessario descrivere nel PTOF quali sono i **motivi didattici** che rendono necessaria la pubblicazione delle fotografie, esplicitando il **fine esclusivo** di "documentare le attività formative", gli **ambienti dove si intende pubblicare** le foto (in un sito, nei social ecc.) e il **grado di privacy applicato** o personalizzato.

Poiché la gestione dell'immagine del minore è tutelata anche dalla legge, è **comunque consigliato farsi rilasciare una liberatoria**, quanto più completa possibile, firmata da entrambi i genitori.

IL REVENGE PORN

Revenge porn è la diffusione sul web di immagini o video privati a sfondo sessuale a scopi vendicativi e senza il consenso della persona ritratta

IL REVENGE PORN

La locuzione di origine anglosassone "revenge porn", o anche "revenge pornography", associa la parola "vendetta" (revenge) a quella di pornografia, lasciando subito intendere la portata del comportamento che la stessa sta a indicare.

La nozione è ormai di uso tristemente comune, complice il moltiplicarsi di episodi di "vendetta porno" ai danni di innumerevoli vittime sia uomini che, prevalentemente, donne che si sono ritrovate violate nella loro sfera intima e hanno visto la propria immagine diffondersi in maniera "virale" senza averlo mai concesso o, addirittura, dopo essere state immortalate a loro insaputa.

Revenge porn: in cosa consiste

Il revenge porn può, dunque, essere identificato nella pubblicazione, o minaccia di pubblicazione (anche a scopo di estorsione), di fotografie o video che mostrano persone impegnate in attività sessuali o ritratte in pose sessualmente esplicite, senza che ne sia stato dato il consenso dal diretto interessato, ovvero la persona o una delle persone coinvolte.

REVENGE PORN

La cronaca ha dimostrato come a perpetrare il ricatto sessuale siano soprattutto persone legate alla vittima da un rapporto sentimentale (coniugi, compagni/e, fidanzati/e), che agiscono in seguito alla fine di una relazione per "punire", umiliare o provare a controllare gli ex facendo uso delle immagini o dei video in loro possesso.

Può trattarsi, ad esempio, di *selfie* scattati dalla stessa vittima ed inviati all'ex partner, oppure di video e fotografie scattate in intimità con l'idea che dovessero rimanere nella sfera privata oppure, addirittura, di scatti e riprese avvenuti di nascosto, senza che una delle parti ne fosse consapevole.

La condivisione di tali immagini, che può avvenire in rete, ma anche attraverso e-mail e cellulari, conduce ad un risultato aberrante per le vittime: umiliazione, lesione della propria immagine e della propria dignità, condizionamenti nei rapporti sociali e nella ricerca di un impiego.

I RICATTI SESSUALI IN ITALIA – I CASI PIU' NOTI

Il fenomeno, purtroppo, ha visto una crescita esponenziale negli ultimi anni anche in Italia dove gli episodi di vendetta pornografica hanno talvolta assunto contorni drammatici, risolvendosi nella morte delle vittime, esasperate dalla situazione creatasi a seguito della diffusione dei proprio video o scatti privati.

Molte vittime di *revenge porn* hanno riferito agli psicologi che l'impatto della diffusione su larga scala di immagini scattate privatamente può essere paragonato a quello di una vera e propria violenza sessuale

Il caso di Tiziana Cantone (2016)

Il pensiero va subito a Tiziana Cantone, giovane donna napoletana i cui video hard avevano iniziato a circolare in rete, ma anche su WhatsApp e poi su Facebook, diffondendosi con quella incontrollabile "viralità" a cui i social ci hanno tristemente abituati. Una vicenda che, nonostante la battaglia legale intrapresa a difesa del proprio diritto all'oblio, si è conclusa con il suicidio della vittima.

Il caso di Giulia Sarti (2018)

La vicenda dell'ex presidente grillina della commissione Giustizia di Montecitorio Giulia Sarti, le cui immagini private sono state diffuse online divenendo presto virali a causa delle incessanti condivisioni, ha assunto i contorni di un vero e proprio caso politico.

Il caso di Giulia Sarti

Un fenomeno che ha portato il Garante per la privacy ad intervenire per richiamare *“l'attenzione dei mezzi di informazione al rispetto della normativa in materia di protezione dei dati personali e del codice deontologico dei giornalisti".*

Inoltre, assieme all'iniziativa dell'Authority, sono giunte numerose e unanimi reazioni di solidarietà nei confronti della deputata da parte di personalità istituzionali ed esponenti di tutte le forze politiche presenti in parlamento.

La maestra di Torino (novembre 2020)

Ultimo in ordine temporale il recente caso di una maestra di Torino che, non è stata solo vittima di *revenge porn* da parte del ex fidanzato, che ha condiviso alcune immagini e video privati della coppia nella chat del calcetto.

In aggiunta è stata ulteriormente vittima delle persone che condividendo a loro volta le immagini, sono arrivati a minacciarla e licenziarla per qualcosa di cui lei era solo una vittima.

La maestra di Torino (novembre 2020)

Infatti la mamma di un bambino alunno della vittima, dopo aver minacciato la maestra qualora avesse sporto denuncia, ha avvertito la dirigente dell'asilo che l'ha licenziata e umiliata, rendendo noti i motivi del provvedimento nonostante nulla avessero a che fare con il suo lavoro.

La direttrice è stata chiamata a processo per diffamazione, l'ex fidanzato della vittima è stato condannato ad un periodo di lavori socialmente utili che durerà un anno. Svolgerà otto ore di servizio a settimana senza poter disporre di sospensioni nei periodi festivi. La maestra ha inoltre chiesto centinaia di migliaia di euro di risarcimento, altrimenti si costituirà parte civile nel processo penale che attende la direttrice e la moglie dell'amico calciatore.

Come difendersi dal revenge porn

Molti paesi, stante le dimensioni sempre più preoccupati che ha assunto il fenomeno, hanno deciso di seguire una linea dura e adottare normative ad hoc per **contrastare e perseguire il revenge porn**: ciò è avvenuto, ad esempio, in Germania, Israele e Regno Unito, e in trentaquattro Stati degli USA.

In Italia, fino all'agosto 2019, non esisteva alcuna legge specifica in materia e l'unica possibilità riconosciuta alle vittime era quella di fare riferimento alla normativa sui reati di diffamazione, estorsione, violazione della privacy e trattamento scorretto dei dati personali.

LA MODIFICA AL CODICE PENALE: IL REVENGE PORN DIVENTE REATO

In Italia con la **legge Codice Rosso** è stato introdotto il **reato di revenge porn** anche nel nostro paese, previsto e punito **dall'art. 612-ter del codice penale.**

Gli intenti sono stati tradotti effettivamente in legge con il c.d. "Codice Rosso", ovvero con le modifiche al codice penale e al codice di procedura penale volte a tutelare le vittime di violenza domestica e di genere introdotte dalla Legge n. 69/2019, in vigore da agosto 2019.

Il reato di revenge porn: art. 612-ter del codice penale

La legge ha introdotto nel codice penale, all'articolo 612-ter, una fattispecie ad hoc, volta a sanzionare il fenomeno del *c.d. revenge porn*.

Si tratta del delitto di diffusione illecita di immagini o video sessualmente espliciti senza il consenso delle persone rappresentate.

ART. 612-ter C.P. - La pena prevista

La nuova fattispecie di reato punisce: "chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde, senza l'espresso consenso delle persone interessate, immagini o video sessualmente espliciti, destinati a rimanere privati - con - la reclusione da 1 a 6 anni e la multa da 5.000 a 15.000 euro".

Si punta a punire anche la condotta degli eventuali "condivisori" delle immagini diffuse dall'autore del reato. La stessa pena, dunque, si applicherà anche nei confronti di chi, avendo ricevuto o comunque acquisito le immagini o i video, li diffonde a sua volta al fine di recare nocumento agli interessati.

Le aggravanti

La fattispecie è aggravata se il reato di pubblicazione illecita è commesso dal **coniuge**, anche separato o divorziato, ovvero da persona che è o è stata legata da **relazione affettiva** alla persona offesa.

Ulteriori aggravanti sono previste anche se i fatti sono commessi **attraverso strumenti informatici** o telematici oppure se sono commessi in danno di persona in condizione di inferiorità fisica o psichica o in danno di una donna in stato di gravidanza.

La procedibilità

Il reato è punibile a **querela della persona offesa**, che potrà essere proposta nel termine di sei mesi e rimessa solo in sede processuale.

La diffusione illecita di video o immagini sessualmente esplicite aggravata in quanto commessa in danno di persona in condizione di inferiorità fisica o psichica o in danno di una donna in stato di gravidanza, è invece **punibile d'ufficio**.

Revenge Porn – Un problema Globale

Secondo uno studio, in Europa circa 9 milioni di ragazze hanno subìto una qualche forma di violenza online prima dei 15 anni. Dopo i mesi di *lockdown* dovuti alla pandemia, si è registrato un netto aumento dei casi di *revenge porn,* termine che indica la diffusione di immagini o video intimi senza il consenso dei protagonisti. L'obbligo di rimanere a casa ha messo a rischio molte persone, soprattutto perché in tanti hanno cominciato a usare strumenti come Zoom o Skype, che offrono nuove occasioni per portare avanti questo genere di abusi.

Le leggi sul *revenge porn* variano molto da un paese all'altro e per gli esperti il diritto non riesce a tenere il passo con le nuove tecnologie.

Differenze con sexting

Diverso dal revenge porn è il sexting.

Quest'ultimo, infatti, consiste nell'invio di messaggi, testi o immagini a sfondo sessuale tramite il cellulare o altri strumenti informatici. Non c'è quindi la diffusione pubblica ma si tratta di uno scambio tra due soggetti, spesso (ma non necessariamente) entrambi consenzienti.

Il termine derivato dalla fusione di sex (sesso) con texting (invio di messaggi elettronici).

Grazie per l’attenzione

dott.ssa Elisa Palermo