Uso degli strumenti web

Proposta di integrazione del Codice comportamentale per i dipendenti del SSR

Linee guida per la redazione di una policy dell'istituzione

Approfondimenti

Gruppo di lavoro
Dott.ssa Sara Salti
Dott.ssa Roberta Caldesi
Dott. Giacomo Galletti

ARS TOSCANA
agenzia regionale di sanità

SOCIAL MEDIA IN AMBITO SANITARIO

Come tutte le istituzioni, anche le organizzazioni che si occupano di salute stanno implementando l'uso dei social media.

Da un **raffronto internazionale**, gli esempi che si possono trarre dall'uso nei sistemi sanitari includono:

- La gestione di una comunicazione individuale e di comunità su un determinato tema (esempio una pagine social monotematica o dedicata ad uno specifico servizio)
- La gestione di un canale social, abbinato al sito istituzionale, al fine di veicolare informazioni su servizi, politiche sanitarie, temi sanitari o di salute di attualità (progetto di comunicazione integrata)
- La sperimentazione di un nuovo modo di comunicare sui temi della salute (promozione dei corretti stili di vita) e ingaggiare nuovi utenti

La scelta di aprire un canale social implica, prima di tutto, una condivisa modalità di approccio allo strumento, nella consapevolezza che anche la "libertà" di utilizzo dello stesso implica una personale responsabilità.

Dall'altra è opportuno condividere una base di conoscenze derivanti dalle implicazioni degli strumenti web che non tutti conoscono.

Alla luce del Codice di Comportamento dei dipendenti pubblici che interessa anche il settore della sanità pubblica e nella prospettiva di "educare" ai principi di una buona "self-communication", è quanto mai opportuno individuare linee di comportamento virtuose sui social.

Queste linee guida, pertanto, pur non avendo la pretesa di essere esaustive sul tema, rappresentano la complessità degli argomenti e le implicazioni di una comunicazione sul web individuale e istituzionale.

Nel tenerne conto, si prefigura una base delle policy da cui l'istituzione deve partire per delineare il campo di azione e dei comportamenti da tenere.

SOCIAL MEDIA - COSA SONO

Con il termine **"Social media"** si intende la gamma dei processi di utilizzazione da parte delle persone **degli strumenti e delle piattaforme on line** (Facebook, Twitter Instagram, la forma del blog, etc) per scambiare contenuti e informazioni generate dagli utenti attraverso conversazioni e scambio di materiale video, fotografico, documentale.

Perciò i social media vengono generalmente utilizzati dalle persone e dalle organizzazioni per:

- **lo scambio interattivo** di informazioni e comunicazioni, dati e conversazioni su diversi temi
- **comunicazioni personali**
- **scambi educativo/informativi** (tematici) soprattutto da parte delle istituzioni o di gruppi di interesse
- **scambio di opinioni**
- **intrattenimento**
- **marketing** (per le aziende e il mercato)

SOCIAL MEDIA: ALCUNE AVVERTENZE

Generalmente l'approccio all'uso del social è molto friendly e l'utente non è consapevole dei rischi che lo strumento ha insiti.

Si seguito si riportano **informazioni** che possono rivelarsi utili ad una corretta impostazione della propria comunicazione sul web.

1) Le informazioni sul web possono essere copiate e diffuse in modo infinito, passando da un profilo all'altro sui social e da un social ad un altro fino a divenire **"virale"** (come si dice in gergo)
2) Non esiste nessuno strumento ad oggi che possa permettere di "cancellare" definitivamente dal web informazioni inavvertitamente inserite: pertanto **la persistenza** è una delle caratteristiche. Il **diritto all'oblio** non è ad oggi totalmente garantito, perché ogni dato, immagine, informazione diramata si diffonde e può restare sul web
3) Altro problema è l'**autenticità dell'informazione**. Attraverso i social non è assolutamente garantita. Chiunque può appropriarsi di una informazione corretta e generarne una verosimile ma

sostanzialmente modificata (fake news), altra rappresenta un "sentito dire", altra ancora è generata, da un superficiale passa parola.

4) **Il furto di identità.** Pochi sanno che la propria immagine è un dato personale che può essere rubato e riutilizzato con la modifica di dati generando un falso, soprattutto se l'utente ha reso in internet altri dati personali quali il codice fiscale o la data di nascita.

SOCIAL MEDIA: COMPORTAMENTO E CONSAPEVOLEZZA PER IL DIPENDENTE E IL PROFESSIONISTA DEL SERVIZIO SANITARIO

I social media rappresentano la **gamma di strumenti** on line che possono essere utilizzati sia per fini personali sia professionali.

Con gli strumenti web quali Facebook, twitter, etc, si assiste di fatto ad una disintermediazione dell'uso dello strumento medesimo: ogni persona è libera di aprire un proprio profilo o realizzare un proprio sito web, un proprio blog per scambiare materiale, informazioni, ospitare punti di vista tematici di altre persone e/o professionisti.

La disintermediazione implica da parte delle persone - di contro ad ogni azione di intermediazione - **la conoscenza delle regole** del mezzo di comunicazione usato e **la consapevolezza delle conseguenze** derivanti dagli obblighi deontologici, regolamentari, normativi ed etici, e i rischi a cui, chi ne fa uso, va incontro.

Questo pone **due questioni etiche** rilevanti per le organizzazioni sanitarie: da una parte di far fronte ad un uso inappropriato di questi strumenti da parte dei dipendenti del sistema, indicando **alcune limitazioni** che in realtà si pongono come vere e proprie **sfide comportamentali**.

Dall'altra l'acquisizione di una consapevolezza sugli effetti collaterali dello strumento e dell'uso friendly che se ne fa.

Sussiste, infatti, la necessità di maturare una seria e provata **consapevolezza**, nell'utilizzo di tali strumenti, per cogliere le tante opportunità offerte dai medesimi e **ridurre**, di contro, al minimo i **numerosi rischi connessi.**

L'ambiente Social, se pur ambiente virtuale, si manifesta come uno spazio "sociale" entro cui le persone si muovono con la differenza che non vi è l'immediata percezione degli errori e pericoli che un comportamento non consapevole dell'uso dello strumento può produrre, conducendo a conseguenze importanti rispetto ad un **comportamento o atteggiamento non etico** o addirittura **riconducibile ad un reato**.

Una rete capace di mettere sullo stesso piano comunicativo Aziende Sanitarie/Professionisti/Persone Assistite/Cittadini, infatti, può dar luogo a fenomeni a volte molto critici. Prova ne sono, ad esempio, **le tante e discutibili immagini** che illustrano momenti di vita quotidiana negli ospedali o sugli scenari di soccorso che giungono direttamente dall'interno di sale operatorie o di camere di degenza degli ospedali. Oppure condivisione di foto, filmati e/o contenuti personali non adeguati al ruolo ricoperto o in contrasto con questo (foto riproducenti feste dove si consumano bevande alcoliche o si manifestano altri comportamenti non consoni al decoro e alla reputazione personale, il linguaggio scurrile, etc).

CONSAPEVOLEZZA NELL'USO DEI SOCIAL

L'uso consapevole dei social e di una corretta "Auto-comunicazione" (self-communication) può portare, invece, dei benefici.

La consapevolezza è un concetto associato alla persona che assume comportamenti etici e legali e, in particolar modo, per la persona che lavora in ambienti molto delicati quale è quello socio-sanitario dove si viene a conoscenza di una serie di informazioni sensibili se non addirittura "sensibilissime" (HIV, mamma segreta, gender, etc), la consapevolezza ricopre un ruolo deontologico.

Tutti i professionisti e i dipendenti del sistema sanitario devono comunque comprendere che il proprio comportamento non è disgiunto rispetto al contesto lavorativo, ma un tutt'uno e pertanto è fondamentale che le organizzazioni del sistema considerino la codificazione di policy o linee guida comportamentali rispetto all'uso dei social media, da ricondurre al **Codice di comportamento** adottato.

Importante e fondamentale è, anche, una corretta **informazione e formazione** sui social e il web in genere.

Le informazioni confidenziali quali quelle che riguardano lo stato sociale e il profilo di salute delle persone hanno garantita la riservatezza e la confidenzialità dei professionisti della sanità pertanto non possono essere trattate sul web.

Alla base di tutto c'è la **conoscenza** delle regole basilari del diritto alla **privacy e la consapevolezza** di essere in possesso di **informazioni confidenziali** che devono essere mantenute a prescindere , in qualsiasi momento della propria vita, evitando di "trattare" impropriamente informazioni personali e sensibili altrui, e quando è necessario farlo, prendere le adeguate precauzioni.

LA SFIDA ETICA NELL'USO DEI SOCIAL DELLE ISTITUZIONI SANITARIE E SOCIO SANITARIE

L'uso dei new media da parte delle istituzioni sanitarie deve trovare una sua **autodisciplina** tenendo conto di quelle che sono:

- **La normativa europea e nazionale** che riguarda il rispetto della liceità del trattamento delle informazioni e dei dati (e quindi delle relazioni) tra struttura sanitaria e paziente, medico e paziente, operatori e utenti
- **Le norme internazionali e le leggi nazionali** riguardanti il rispetto dei diritti degli individui
- **Le regole deontologiche** dei professionisti della sanità
- **Il codice di comportamento** (o più propriamente un'etica comportamentale) dei propri dipendenti rispetto all'attività e rispetto all'azienda/istituzione

Le questioni che ne derivano sono pertanto di due tipi:

- ➔ la prima riguarda **il comportamento pubblico sul web tenuto da persone appartenenti al Sistema.** In quanto professionisti, oltre che dipendenti di un'azienda e appartenenti ad un Sistema, il comportamento incide non solo sui principi di "sicurezza" dei cittadini/utenti, ma anche rispetto alla propria **reputazione personale e professionale** e per la **"reputazione" dell'azienda e del sistema**. Il comportamento della persona-dipendente deve assumere una connotazione di forte consapevolezza degli atti comunicativi e dei contenuti scambiati liberamente anche come privato cittadino. Tale implicazione porta alla redazione di **regole comportamentali aggiuntive nel codice di comportamento** che non sarebbe male potesse essere un codice di comportamento del SSR se non addirittura del SSN
- ➔ la seconda riguarda la **policy** che l'azienda o il sistema definisce per come ci si pone attraverso gli strumenti web che il sistema e/o l'Azienda ha inteso istituire e che deve contenere norme comportamentali dei dipendenti che sono abilitati ad utilizzare quegli strumenti, a tutela dei diritti di privacy, diritti dei pazienti/utenti, segreto di ufficio etc.

Il processo di **creazione di consapevolezza delle persone** che lavorano nel sistema sanitario investe, pertanto, due ambiti a cui si possono ricondurre le linee guida che, pertanto, sono di due tipi:

- una riguardante **un codice etico (individuale), sull'uso dei social media,** da inserire nel codice di comportamento.

- una riguardante **le regole per una gestione appropriata degli strumenti social** in ambito aziendale e di sistema sanitario.

LINEE GUIDA PER L'INTEGRAZIONE DEL CODICE DI COMPORTAMENTO SUI SOCIAL MEDIA

I principi deontologici verso cui si deve conformare il dipendente del sistema sanitario si rispecchiano anche sul web: basti pensare quanto previsto per il **decoro personale** e la **salvaguardia del prestigio** della professione.

Per usare in modo appropriato i social media e averne il più possibile un beneficio rispetto alle attività dell'organizzazione sanitaria e del sistema stesso, **una seria politica sul web** deve prevedere **regole scritte**, **formazione** e **discussione** con i professionisti che ne fanno uso.

Per il settore sanitario e socio-sanitario in cui vengono trattati dati sensibili (vedi codice privacy) l'uso dei social rappresenta anche un problema di **sicurezza**.

Il concetto base su cui si muovono i social, infatti, e che riguarda l'auto-comunicazione (self-communication, approccio diretto senza mediazione) e la libertà di espressione, a partire dalla divulgazione di immagini (anch'esse dato sensibile in quanto legate oltre che alla propria sfera privata, all'identità) sembra cozzare con i principi e le buone regole della riservatezza.

Prima dell'avvento dei social, a partire dalle mail fino agli sms, ogni comunicazione era consapevolmente gestita da uno a molti, quando i molti erano (sono) persone definite e scelte in una cerchia di interessi a cui mail e sms sono diretti.

Con i social, a meno che non si determini un profilo chiuso tra persone (club), chiunque può accedere e vedere le stesse informazioni anche se non sono direttamente di proprio interesse o contestualizzate.

Questo oggettivamente provoca una "diffusione di informazioni" incontrollata.

Coloro che lavorano nel settore sociale e sanitario inavvertitamente o di proposito possono divulgare dati di pazienti o informazioni sensibili a partire dalla immagini, ad esempio, che possono avere effetti devastanti su quella persona o per l'azienda o lo stesso sistema. Oltre che violare norme cogenti.

Al fine di redigere **un codice etico sull'uso dei social media** che sia inglobato nel Codice di Comportamento dei dipendenti, bisogna tenere conto delle fonti normative vigenti in Italia e riguardanti i doveri del lavoratore del pubblico impiego.

I **doveri del dipendente**, in particolare, possono essere raggruppati in due ampie tipologie:

- una di stampo prettamente **pubblicistico**, riconducibile al dovere di fedeltà alla Repubblica, sancito dall'art. 51 Cost., ai principi di

imparzialità e buon andamento, ex art. 97 Cost., e al carattere democratico della Repubblica (art. 1 Cost.), che impone di favorire rapporti di fiducia fra amministrazione e cittadino.

- l'altra richiama i **doveri di diligenza**, **obbedienza e fedeltà** sanciti, come per il rapporto di lavoro privato, dagli artt. 2104 e 2105 dl Codice Civile e che, per il pubblico impiego, trova esplicitati nel codice di comportamento «uniforme» per tutte le amministrazioni pubbliche e coordinato con le previsioni contrattuali in materia di responsabilità disciplinare.

Le **Fonti del diritto**, riguardanti il comportamento del personale afferente ai sistema sanitario pubblico, nel nostro paese, ad oggi sono:

- Il D.P.R. 16-4-2013, n. 62, adottato in base alla L. 190/2012
- l'art. 28 del CCNL comparto sanità del 1 settembre 1995
- Codice deontologico dei medici odontoiatri
- Codici deontologici delle singole professioni sanitarie (infermieri, psicologi, logopedisti, ostetriche, veterinari, farmacisti, assistenti sociali, biologi, chimici, etc)
- Codice deontologico giornalisti

In sostanza e in estrema sintesi, tutte queste norme esplicitano **tre aspetti** del comportamento virtuoso nei confronti dell'amministrazione per cui il dipendente lavora e riguardo al comportamento da tenere in ambienti non lavorativi:

1) Evitare comportamenti e situazioni che possano nuocere alla **reputazione propria e a quella** della pubblica amministrazione per cui lavora
2) perseguire il **segreto di ufficio** nel rispetto delle disposizioni in materia di trasparenza e di accesso all'attività amministrativa
3) attenersi alle disposizioni del **codice privacy**

Questi tre aspetti rappresentano la necessità di assumere basi comuni di conoscenza e di comportamento per tutti coloro che sono dipendenti del Sistema Sanitario e che sui social si identificano o vengono identificati, conosciuti o si muovono come appartenenti al sistema aziendale / dello stesso sistema.

Di seguito sono pubblicati i contenuti minimi per l'integrazione del Codice di Comportamento e la netiquette. A parte, l'allegato 3 riporta la scaletta delle informazioni per redigere la social media policy aziendale.

ALLEGATO 1

CODICE DI COMPORTAMENTO DIPENDENTI PUBBLICI
LINEE COMPORTAMENTALI PER L'USO DEL WEB

Linee comportamentali

A. I dipendenti del Servizio sanitario ...(indicare azienda/ente/etc) devono attenersi alle leggi, ai rispettivi codici deontologici e al codice di comportamento ed etico riferiti al pubblico impiego e adottato dalle aziende del sistema, e tenerne conto nel momento in cui interagiscono su un Social Media

B. Salvo il diritto di esprimere valutazioni e diffondere informazioni a tutela dei diritti sindacali, ben rappresentando questo tipo di opinione, il dipendente si astiene da dichiarazioni pubbliche offensive nei confronti dell'amministrazione, osserva il segreto di ufficio e la normativa ai sensi della privacy

C. L'azienda/ ente/…….. si aspetta dai suoi dipendenti che riflettano i valori dell'azienda/ente/……. quando postano in un social un contenuto circa la politica aziendale/ etc…..

D. Il dipendente che posta contenuti attinenti all'attività aziendale/ ……. è personalmente responsabile di ciò che inserisce sul social utilizzato

E. E' vietata la diffusione, in qualsiasi forma e attraverso qualunque media e social media, di informazioni riservate e informazioni identificative personali di cui ne sia venuti a conoscenza con il proprio lavoro

F. E' vietata la diffusione in qualsiasi forma e attraverso qualunque media e social media di informazioni confidenziali provenienti dall'attività clinica e assistenziale;

G. I dipendenti……. evitano, in qualunque strumento web utilizzato, un comportamento di scherno o discriminatorio sia verso persone che verso altri dipendenti del sistema

H. I dipendenti del…….. rispettano il diritto alla privacy dei pazienti, utenti dei servizi e colleghi evitando di postare foto, immagini o descrizioni che non siano preventivamente autorizzate per iscritto dagli stessi pazienti, utenti dei servizi e colleghi. I dipendenti devono tenere presente che il diritto alla privacy può essere violato quando il post nel Social Media contiene abbastanza dettagli del paziente, utente del servizio o collega tali da essere identificati

I. I dipendenti del …….. non devono screditare sul web i servizi e le cure che i pazienti e i cittadini ricevono. Tale violazione è più seria quando i pazienti e i cittadini hanno accesso ai post del social

media utilizzato, e in particolar modo quando pazienti e cittadini risultano essere amici nella pagina personale del dipendente come può essere quella di facebook

J. I dipendenti del …… devono preventivamente ottenere l'autorizzazione scritta per postare loghi, foto, video o immagini riferite alle aziende o attività del sistema sanitario nel proprio sito/pagina personale

K. Contraenti e fornitori del sistema sanitario e delle aziende sono soggetti alle stesse regole e divieti quando decidono di postare sui social media informazioni riferite alle stesse aziende e al sistema

Tali linee comportamentali non si applicano ai contenuti attinenti alla sfera privata.

ALLEGATO 2

NETIQUETTE

Il termine **"netiquette"** rappresenta l'insieme delle regole che delineano i parametri di educazione e buon comportamento (dal francese *etiquette*) da tenere in Rete (dall'inglese *net*).

Si tratta di regole del "buon comportamento" quando si usa internet, che se pur realizzate e auspicate già dagli esordi del web, spesso non sono conosciute o comunque dimenticate.

La netiquette è fondamentale come linea guida per un comportamento individuale, del privato cittadino, accettabile in rete.

Di seguito solo alcuni punti cardine per delineare la netiquette, a partire dalla considerazione che il web non è un "altro mondo", è solo un "altro strumento" e le azioni scorrette sono passibili di denunce e procedimenti penali. La persona dovrebbe comportarsi esattamente come le regole civili richiedono nella vita di tutti i giorni.

Linguaggio

- Scrivere correttamente prestando attenzione all'ortografia e alla punteggiatura. Tutti vedono gli scritti (leggere il messaggio tre volte prima di pubblicarlo).
- Le parole hanno un valore e, pertanto, un peso: essere fraintesi è facile. Usare parole che hanno un significato ambiguo o che, ancora peggio, istigano all'odio, alla discriminazione o indicano un forte pregiudizio specialmente su altre persone può essere considerato anche un reato
- Scrivere con caratteri MAIUSCOLI sul web, per convenzione, equivale ad URLARE
- Usare le faccine per dare il tono a quello che viene scritto deve essere fatto con complementarietà di significato altrimenti può risultare offensivo

Privacy

- Non pubblicare informazioni personali e dati sensibili di altri utenti.
- Richiedere il consenso prima di taggare gli altri su foto o video
- Non pubblicare foto che potrebbero mettere in imbarazzo un'altra persona

Copyright

- Se si sceglie di pubblicare testi, foto o video provenienti da altri siti web va riportata la fonte. Meglio se si mette un link per rendere raggiungibile la fonte.

Stile comunicativo

- Quando si lascia un **commento**, devono essere rispettati i valori, il credo e i sentimenti degli altri e non attaccare a livello personale gli autori degli articoli pubblicati.
- Si può esprimere la propria **posizione** in modo rispettoso, anche se non si è d'accordo con il parere di chi scrive o il suo stile di scrittura
- Entrare in una **discussione** serve a portare un valore aggiunto, scrivere qualcosa che abbia senso all'interno di quella discussione e non per accendere litigi e offendere.
- Invitare i tuoi contatti ad **applicazioni**, giochi, pagine selezionando quelli che potrebbero essere realmente interessati ai tuoi interlocutori
- Usare gli **hashtag** in modo corretto (ne basta uno!) per rendere facilmente rintracciabile quello che scrivi per chi è interessato ad un particolare argomento

ALLEGATO 3

LINEE GUIDA PER LA REDAZIONE DI UNA SOCIAL MEDIA POLICY ISTITUZIONALE

1. Apertura di un canale social

- registrazione del profilo attraverso un contratto ad oggetto informatico con firma del contratto del vertice
- Lettura dei termini del servizio che devono essere accettati dall'Ente prima di poter accedere ai servizi di social media e prima della creazione del profilo.
- Tali condizioni, che è opportuno conservare al pari di qualunque altro contratto, si occupano di:

  privacy policy

  condotte consentite all'utente

  diritti sui contenuti inseriti dagli utenti

  limitazioni di responsabilità del fornitore
- attenzione al tipo di comportamenti vietati dal gestore
- diritto d'autore e proprietà contenuti pubblicati dall'ente

2. Redazione di una social policy è il documento destinato al personale interno che regola il rapporto tra l'organizzazione dell'ente e la gestione del social media e deve prevedere due tipologie di indicazioni:

➔ **generali**: riguardanti la modalità della presenza, il comportamento dei dipendenti nella gestione della presenza on line, la filosofia degli interventi, le linee editoriali etc

➔ **specifiche** che sono:

- l'indicazione dell'ufficio (o struttura) che si occupa della gestione del profilo dell'ente (pubblicazione contenuti, interazione con gli utenti, monitoraggio degli aggiornamenti dei termini di servizio, etc)
- precisazione di quali contenuti possono essere pubblicati e con quale tipo di licenza
- informazione dei dipendenti sull'attività dell'Ente sui social e modalità di interazione con i vari settori
- definire le cautele in materia di sicurezza (es. password di accesso)

Il documento di social media policy interna conterrà informazioni sull'uso di rappresentanza dell'Ente (chi è abilitato al profilo e come agisce); le indicazioni sul codice di comportamento del personale e le modalità di gestione degli account e, non ultima, la gestione dei contenuti.

Il documento di social media policy esterna illustrerà le regole di comportamento da parte dell'utenza, i cui contenuti minimi devono essere

- Ente e ufficio che gestisce lo spazio
- finalità perseguite dall'Amministrazione con il social
- tipo di contenuti pubblicati, argomenti e temi e tipologie escluse (ai sensi privacy, etc)
- informativa ai sensi della privacy
- se trattasi di social che sviluppa un dialogo con i cittadini valutazione e ammissione dei post, tempi di risposta, cosa viene postato e cosa viene non postato
- uso degli hashtag
- se connesso o meno con le informazioni sul sito istituzionale
- se riporta o meno anche altre fonti e come queste vengono rappresentate
- accenno alla gestione o meno del diritto di autore, marchi registrati, pubblicità etc
- netiquette

APPENDICE

IL CODICE DI COMPORTAMENTO DEI DIPENDENTI DELLE PUBBLICHE AMMINISTRAZIONI

Il codice definisce i **doveri minimi di diligenza, lealtà, imparzialità e buona condotta** che i pubblici dipendenti sono tenuti ad osservare.

Ciascun dipendete deve servire la nazione con disciplina ed onore, conformando la propria condotta ai principi di buon andamento e di imparzialità nell'azione amministrativa.

Deve svolgere i propri compiti nel rispetto della legge, perseguendo l'interesse pubblico senza abusare della propria posizione, rispettando i principi di integrità, correttezza, di buona fede, proporzionalità, obiettività, trasparenza, equità e ragionevolezza ed agire in posizione di indipendenza ed imparzialità, astenendosi dal conflitto di interessi.

Del Codice di Comportamento **gli articoli che seguono** in particolare **sono anche riferibili a processi comunicativi personali e all'uso di strumenti per la comunicazione.**

L'art. 3 prevede che il dipendete non utilizzi ai fini privati le informazioni di cui dispone per ragioni di ufficio, evita situazioni e comportamenti che possono ostacolare il corretto adempimento dei compiti o nuocere agli interessi e all'immagine della pubblica amministrazione.

L'art. 11 disciplina l'utilizzo del materiale sanitario in quanto stabilisce che il dipendente utilizzi il materiale o le attrezzature di cui dispone per ragione di ufficio e dei servizi e telefonici telematici (telefono, internet, email) nel rispetto dei vincoli posti dall'amministrazione .

L'art. 12 prevede che il dipendente operi con spirito di servizio, correttezza, cortesia e disponibilità, salvo il diritto di esprimere valutazioni e diffondere informazioni a tutela dei diritti sindacali, si astenga da dichiarazioni pubbliche offensive nei confronti dell'amministrazione. Si prevede altresì che osservi il segreto di ufficio e la normativa in materia di tutela e trattamento di dati personali.

LA RESPONSABILITA' PROFESSIONALE E DEONTOLOGICA

Il codice deontologico per gli ordini professionali del settore sanitario e sociale che ne hanno approvato un testo, fissa generalmente le norme dell'agire professionale e definisce i principi guida che strutturano il sistema etico in cui si svolge la relazione con la persona assistita o tra gli stessi professionisti.

Lo scopo è quello di aumentare la responsabilità del personale sanitario che si concretizza nell'assistere, curare e prendersi cura della persona nel

rispetto della vita della salute, della libertà e della dignità dell'individuo, sottolineando la necessità di una responsabilità sociale a fronte del ruolo ricoperto.

Di seguito sono indicati gli articoli e i punti salienti in fatto di comunicazione e/o informazione estrapolati dai codici deontologici delle principali professioni in ambito sanitario (medici e infermieri) e sociale (assistenti sociali).

MEDICI

Sotto il profilo deontologico il **Codice di Deontologia Medica** pone specifiche regole di condotta che devono orientare l'iscritto non solo nella diretta comunicazione con i pazienti, ma anche nell'uso di strumenti di comunicazione a cui possono essere ricondotti per analogia anche i social media.

Rilevante è la prescrizione dell'art. 1, comma 3, secondo cui "*Il Codice regola anche i comportamenti assunti al di fuori dell'esercizio professionale quando ritenuti rilevanti e incidenti sul decoro della professione*".

Gli artt. 10,11,12 entrano nel merito del comportamento del medico su segreto professionale, riservatezza dei dati personali e trattamento dei dati sensibili riferiti ai propri pazienti, mentre l'art. 20 sancisce il rispetto dei diritti fondamentali della persona.

Da porre attenzione agli articoli 55, 56 e 57 in quanto esprimono concetti di pubblicità e comunicazione della propria professione che possono trovare negli strumenti del web un canale comunicativo, del tutto equiparabile agli altri mass media (tv, radio, giornali).

Infine occorre porre attenzione all'art. 58 primo degli articoli del codice deontologico che fa riferimento ai rapporti con i colleghi: il medico ha l'obbligo deontologico di preservare il decoro della categoria e di relazionarsi con i colleghi con rispetto e solidarietà, che costituiscono principi cardine della deontologia professionale la cui violazione apporta un indubbio discredito alla stessa dignità della professione.

INFERMIERI

Nel Codice Deontologico di Infermieristica attualmente non vi sono riferimenti specifici agli strumenti di comunicazione e pertanto neppure sui social media. È possibile però, dalla lettura e analisi del predetto Codice, ricavare una serie di riferimenti che permettono di affrontare le questioni legate alla correttezza nella comunicazione:

- Articolo 23: «L'infermiere riconosce il valore dell'informazione integrata multiprofessionale e si adopera affinché l'assistito disponga di tutte le informazioni necessarie ai suoi bisogni di vita»;
- Articolo 26 : «L'infermiere assicura e tutela la riservatezza nel trattamento dei dati relativi all'assistito. Nella raccolta, nella gestione e nel passaggio di dati, si limita a ciò che è attinente all'assistenza»;
- Articolo 27: «L'infermiere garantisce la continuità assistenziale anche contribuendo alla realizzazione di una rete di rapporti interprofessionali e di una efficace gestione degli strumenti informativi»;
- Articolo 46: «L'infermiere si ispira a trasparenza e veridicità nei messaggi pubblicitari, nel rispetto delle indicazioni del Collegio professionale».

La Federazione Nazionale Infermieri nel 2013 ha comunque emanato un documento guida sui social ricavato dalle esperienze internazionali in materia. I punti più salienti sono:

- «prima di postare informazioni online considerare la solidità delle ragioni per farlo, assicurarsi di avere il consenso dell'assistito, che la sua identità sia protetta e che le informazioni pubblicate online non ne permettano l'identificazione»;
- «non diffondere mai attraverso i social media immagini o informazioni relative all'assistito che possano violare i suoi diritti di privacy e riservatezza;»
- «non pubblicare, condividere o diffondere immagini, dati o informazioni dell'assistito acquisite nella relazione infermiere – paziente»;
- «non esprimere commenti sugli assistiti anche quando gli stessi non possono essere identificati»;
- «non acquisire immagini (fotografie, video) utilizzando dispositivi personali ivi inclusi i telefoni cellulari».

Molto più cogenti sono le norme oltreoceano.

L'American Nurses Association, che conta 3,6 milioni di iscritti, ha proposto nel 2011 alcuni principi di buon uso dei social media e dei suggerimenti di base rivolti agli infermieri per non commettere errori o illeciti nell'utilizzare questi strumenti. Secondo tali principi, gli infermieri devono:

- evitare di trasmettere o mettere online informazioni che possono favorire l'identificazione del paziente;
- osservare i principi deontologici e rispettare i confini professionali;
- essere consapevoli che i pazienti, i colleghi, le istituzioni e i datori di lavoro possono visualizzare i loro messaggi;

- impostare correttamente le opzioni dei social media relative alla privacy e mantenere separate le informazioni personali da quelle professionali;
- segnalare alle autorità competenti eventuali contenuti presenti sui social media che possono danneggiare la privacy, il benessere, i diritti degli assistiti o dei colleghi;
- partecipare allo sviluppo di politiche istituzionali che disciplinino la condotta online.

I suggerimenti sono i seguenti:

- far valere gli standard professionali anche per la condotta online o in qualsiasi altra circostanza;
- non condividere o pubblicare informazioni o immagini ottenute attraverso la relazione tra l'infermiere e il paziente;
- non fotografare o girare video di pazienti utilizzando dispositivi personali compresi i telefoni cellulari;
- mantenere i confini professionali;
- non fare commenti su pazienti, colleghi o datori di lavoro anche se non sono direttamente identificati.

ASSISTENTI SOCIALI

Il mandato professionale dell'assistente sociale deriva dal tessuto etico-deontologico e metodologico della professione.

Il Codice deontologico è costituito dai principi e dalle regole che gli assistenti sociali devono osservare e far osservare nell'esercizio della professione che orientano le diverse scelte di comportamento nei diversi livelli di responsabilità in cui operano (art. 1).

Dal Codice emerge chiaramente che la professione si pone al servizio del bene comune, collocando al centro dell'intervento la persona e il comportamento professionale deve aver come scopo prioritario l'interesse e la tutela dei diritti dell'utente.

Come si evince dagli articoli della Parte II del Codice la responsabilità deontologica si profilano, al riguardo, due aspetti: tutela della privacy e segreto professionale.

Quindi:

Art. 23. La riservatezza ed il segreto professionale costituiscono diritto primario dell'utente e del cliente e dovere dell'assistente sociale, nei limiti della normativa vigente.

Art. 24. La natura fiduciaria della relazione con utenti o clienti obbliga l'assistente sociale a trattare con riservatezza le informazioni e i dati riguardanti gli stessi, per il cui uso o trasmissione, nel loro esclusivo

interesse, deve ricevere l'esplicito consenso degli interessati, o dei loro legali rappresentanti, ad eccezione dei casi previsti dalla legge.

Art. 25. L'assistente sociale deve adoperarsi perché sia durata la riservatezza della documentazione relativa agli utenti ed ai clienti, in qualunque forma prodotta, salvaguardandola da ogni indiscrezione, anche nel caso riguardi ex utenti o clienti, anche se deceduti. Nelle pubblicazioni scientifiche, nei materiali ad uso didattico, nelle ricerche deve curare che non sia possibile l'identificazione degli utenti o dei clienti cui si fa riferimento.

Art. 26.L'assistente sociale è tenuto a segnalare l'obbligo della riservatezza e del segreto d'ufficio a coloro con i quali collabora, con cui instaura rapporti di supervisione didattica o che possono avere accesso alle informazioni o documentazioni riservate.

Art. 27. L'assistente sociale ha facoltà di astenersi dal rendere testimonianza e non può essere obbligato a deporre su quanto gli è stato confidato o ha conosciuto nell'esercizio della professione, salvo i casi previsti dalla legge.

Art. 28. L'assistente sociale ha l'obbligo del segreto professionale su quanto ha conosciuto per ragione della sua professione esercitata sia in regime di lavoro dipendente, pubblico o privato, sia in regime di lavoro autonomo libero professionale, e di non rivelarlo, salvo che per gli obblighi di legge e nei seguenti casi:

- rischio di grave danno allo stesso utente o cliente o a terzi, in particolare minori, incapaci o persone impedite a causa delle condizioni fisiche, psichiche o ambientali;

- richiesta scritta e motivata dei legali rappresentanti del minore o dell'incapace nell'esclusivo interesse degli stessi;

- autorizzazione dell'interessato o degli interessati o dei loro legali rappresentanti resi edotti delle conseguenze della rivelazione;

- rischio grave per l'incolumità dell'assistente sociale.

Art. 29. La collaborazione dell'assistente sociale alla costituzione di banche dati deve garantire il diritto degli utenti e dei clienti alla riservatezza, nel rispetto delle norme di legge.

Art. 30. L'assistente sociale nel rapporto con enti, colleghi ed altri professionisti fornisce unicamente dati e informazioni strettamente attinenti e indispensabili alla definizione dell'intervento.

Art. 31. Nei rapporti con la stampa e con gli altri mezzi di diffusione l'assistente sociale, oltre che ispirarsi a criteri di equilibrio e misura nel rilasciare dichiarazioni o interviste, è tenuto al rispetto della riservatezza e del segreto professionale.

Art. 32. La sospensione dall'esercizio della professione non esime l'assistente sociale dagli obblighi previsti dal Capo III del presente Titolo ai quali è moralmente e giuridicamente vincolato anche in caso di cancellazione dall'Albo.

RESPONSABILITA' - CONCETTO E TIPOLOGIE

Il **concetto di responsabilità** indica il dovere che grava su chiunque di rispondere delle proprie azioni.

Secondo il Diritto la responsabilità consiste nelle «*conseguenze personali e/o patrimoniali a cui va incontro il soggetto che assume un comportamento attivo o passivo (omissivo), che sia lesivo di un interesse tutelato dalla legge.*»

La responsabilità penale deriva dalla violazione di una norma di legge o di una norma di diritto.

Per la configurazione di un reato occorre valutare quali siano gli elementi di reato: il fatto, l'antigiuridicità del fatto, l'elemento psicologico. Nella gradazione del reato occorre considerare: il nesso causale (rapporto tra azione/omissione ed evento) e l'elemento psicologico della condotta (solo o colpa).

La responsabilità civile consiste nell'obbligo risarcitorio di chi ha causato un danno ingiusto e si suddivide in responsabilità contrattuale ed extracontrattuale. Il danno arrecato può essere considerato patrimoniale (direttamente monetizzabile) non patrimoniale (valutato in via equitativa dal giudice).

Il diritto distingue due differenti tipi di colpa: **specifica** (che deriva dall'inosservanza di leggi, norme regolamenti o discipline) e **generica** (nelle declinazioni di negligenza – il non fare qualcosa che doveva essere fatto in una determinata circostanza- imprudenza – l'aver posto in essere un comportamento che non doveva essere posto in una determinata circostanza, imperizia – l'aver agito senza la dovuta perizia, ossia quella competenza tecnico-scientifica specifica, necessaria per porre un determinato comportamento).

Sanzioni

Sotto il profilo della violazione del codice deontologico è utile distinguere fra sanzioni disciplinari e deontologiche. Le prime si sostanziano in: biasimo orale, biasimo scritto, multa, sospensione, licenziamento; mentre le seconde sono: avvertimento, censura sospensione e radiazione.

SEGRETO PROFESSIONALE

Ai sensi dell'art. 622 del Codice penale, l'**obbligo del segreto professionale** si riferisce a «*qualsiasi notizia non aperta alla conoscibilità di chiunque (segreto) di cui una persona venga a conoscenza per ragione del proprio stato od ufficio, o della propria professione od arte*».

Quindi l'obbligo di non rivelare il segreto sussiste non solo per chi esercita una professione, ma anche (e a maggior ragione) per altre figure che si trovano in rapporto fiduciario con gli utenti, ad esempio i volontari.

Tuttavia l'obbligo di non rivelare il segreto sussiste solo se si viene a conoscenza di tale segreto durante l'esercizio di una certa professione o durante l'attività di volontariato. Alcune informazioni sono pertanto da tutelare se non sono utili al tipo di aiuto che mettono in atto questi soggetti o al ruolo che ricoprono nel progetto rivolto alla persona.

Le informazioni professionali condivise con i volontari e altri professionisti è opportuna purché si tratti di informazioni strettamente necessarie al tipo di coinvolgimento degli stessi.

La domanda da farsi è quindi: questa informazione è utile per il ruolo di questa persona?

IL CONCETTO DI ILLECITO

Il concetto di illecito indica un comportamento contrario all'ordinamento giuridico che si sostanzia nella violazione di un dovere o di un obbligo imposto da una norma giuridica.

Nell'ordinamento italiano esistono tre tipologie di illeciti: civili, penali, amministrativi.

Gli **illeciti civili** consistono in una violazione di una norma posta a tutela di un interesse privato alla quale consegue una sanzione risarcitoria.

Gli illeciti civili si suddividono in contrattuali e extracontrattuali a seconda della fonte da cui derivi la responsabilità (art. 1218 c.c. e art. 2043 c.c.).

Gli **illeciti penali** (reati) sono costituiti dalle condotte che violino le norme poste a tutela dell'interesse pubblico e si suddividono in delitti e contravvenzioni a seconda della tipologia di sanzione che l'Ordinamento ricollega alla condotta illecita:

- Delitti: alla cui commissione segue l'applicazione di una sanzione fra a) ergastolo, b) reclusione,c) multa;
- Contravvenzioni : alla cui commissione segue l'applicazione di una sanzione fra a) arresto, b) ammenda.

Gli **illeciti amministrativi** sono modellati sulla struttura dei reati, ma sono sanzionati dalla pubblica amministrazione e non dall'autorità giudiziaria. Prevedono l'applicazione di sanzioni pecuniarie che possono

poi essere accompagnate anche da misure accessorie di diversa natura quali i provvedimenti disciplinari.

ILLECITI E SOCIAL MEDIA

Nell'analizzare i rapporti intercorrenti tra illecito e social network è necessario fare la seguente distinzione preliminare:

- illeciti commessi **dai** social network;

- illeciti commessi **tramite o all'interno** dei social network.

Illeciti commessi dai social network

In questa categoria si fanno rientrare quegli illeciti che vengono commessi dalle società che possiedono e gestiscono la piattaforma. Possono essere:

- illeciti societari autonomi;

- illeciti connessi al servizio di social networking offerto.

Negli illeciti connessi al servizio di social networking possiamo individuare tre figure di responsabilità:

il social network come autore dell'illecito (trattamento illecito di dati, illeciti contrattuali sui servizi offerti, ecc.)

- il social network come concorrente nell'illecito (mediante azione o omissione/negligenza)

In altri termini la responsabilità in oggetto si sostanzia nell'assenza di un obbligo di controllo preventivo sui contenuti caricati dagli utenti da un lato e dall'altro nella loro responsabilità nei casi di mancato intervento dopo la segnalazione di un illecito (civile o penale), come ad esempio la rimozione di filmati o foto.

Illeciti commessi tramite o all'interno dei social network

Possono scaturire da tre fattispecie:

- Utilizzo illecito del social network che travisa le funzioni della piattaforma;

- Utilizzo illecito del social network che non travisa le funzioni della piattaforma;

- Utilizzo lecito del social network considerato illecito dall'ordinamento.

VIOLAZIONE DEL DIRITTO DI AUTORE

In tema di responsabilità civile extracontrattuale merita un cenno anche la **violazione del diritto d'autore**.

Il diritto d'autore è tutelato dalla legge n. 633 del 22 aprile 1941 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" nonché dal Titolo IX del Libro Quinto del Codice civile italiano.

Le violazioni del diritto d'autore possono comportare conseguenze sia in sede civile che penale.

Da un **punto di vista civilistico** la violazione del diritto d'autore comporta una responsabilità di natura risarcitoria. L'aspetto che viene tutelato è il c.d. diritto allo sfruttamento economico dell'opera.

Nello specifico, i principali strumenti messi a disposizione dal legislatore in sede civile sono:

1. Azioni di accertamento cautelare e con funzione inibitoria.

2. Azioni per la distruzione o rimozione della violazione

3. Azione per il risarcimento del danno.

4. Azioni strumentali all'esercizio delle difese civili ex art. 161 LDA (Legge Diritto D'Autore Legge 22 aprile 1941, n. 633, "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" e ss.mm.)

In **materia penale** la violazione del diritto d'autore è considerata un «delitto» con pene detentive che, nei casi più gravi, arrivano ai 3 anni di reclusione.

A disciplinare tali aspetti è la stessa Legge sul Diritto d'Autore che dall'art. 171 ss. riporta le singole fattispecie nonché le relative pene detentive e pecuniarie.

Per quanto riguarda l'aspetto social network invece: «*Il gestore di un social network non è tenuto a predisporre un sistema di filtraggio delle informazioni per prevenire la violazione dei diritti d'autore.*» (cfr. Corte di Giustizia Europea Sez. III 360 del 16 febbraio 2012).

L'utente sarà comunque responsabile delle proprie condotte e, oltre alle conseguenze giuridiche, potrebbe essere escluso dall'utilizzo del social network in caso di violazione dei diritti d'autore altrui.

In sede penale si è stabilito che sia «*da ritenersi penalmente responsabile chiunque diffonda anche solo parzialmente opere protette attraverso la pubblicazione delle stesse su social network senza citarne espressamente il coautore» e che sia sufficiente il dolo generico per la configurazione dell'illecito*» (cfr. Tribunale di Genova sez. I 3443 del 13 luglio 2012).

DIRITTO ALL'OBLIO

E' una particolare forma di garanzia, sviluppatasi con l'evoluzione del Web in senso 2.0. Può essere tradotta nel "*diritto a non restare indeterminatamente esposti ai danni ulteriori che la reiterata pubblicazione di una notizia può arrecare all'onore e alla reputazione, salvo che, per eventi sopravvenuti, il fatto precedente ritorni di attualità e rinasca un nuovo interesse pubblico all'informazione*".

In particolare, il diritto all'oblio è ricompreso nei c.d. diritti inviolabili, ossia in quei diritti che pur non avendo esplicito riconoscimento costituzionale, sono comunque garantiti da disposizioni a carattere generale.

In Italia, la sua tutela è garantita dall'art. 2 della Costituzione, secondo cui "*La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità*".

Il diritto all'oblio è riconosciuto anche dalla Suprema Corte, che – da ultimo – nel 2013 ha affermato che: "*per reiterare legittimamente notizie attinenti a fatti remoti nel tempo, è necessario il rilevante collegamento con la realtà attuale e la concreta utilità della notizia, da esprimersi sempre nei vincoli della c.d. continenza espositiva*" (cfr. Cass. Civ. Sez. III1611/13).

L'organo di tutela principale è il Garante della Protezione dei Dati Personali, che è un'autorità amministrativa indipendente. Il Garante non è competente per le richieste di risarcimento danni, che sono invece affidate ai Tribunali Ordinari.

All'interno dei social network , le violazioni del diritto all'oblio potranno essere compiute:

- da singoli utenti, tramite la pubblicazione di una notizia all'interno dello spazio personale che la piattaforma mette a disposizione degli iscritti (ad es. bacheca). In tal caso la rimozione si chiederà allo stesso social network mediante segnalazione.
- dalle pagine pubbliche o profili social dei quotidiani sempre presenti sui social network che si occupano della continua pubblicazione delle notizie. In tal caso la rimozione si chiederà, in primis, direttamente alle teste giornalistiche. Sarà comunque necessario chiedere ai principali motori di ricerca la deindicizzazione dei collegamenti agli articoli illecitamente pubblicati tramite i social network (e non).

CASI RECENTI

Si ricorda il recente caso di un padre che ha pubblicato su Facebook la foto del figlio vittima di bullismo e anche quello della diciottenne austriaca che, dopo aver invano chiesto ai genitori di cancellare le sue foto pubblicate sui loro profili, si è rivolta a un giudice per ottenerne la rimozione.

La veloce circolazione delle fotografie pubblicate sui social network (viralità), senza il preventivo consenso dell'interessato, la circostanza che sono materiali potenzialmente accessibili a tutti, quindi utilizzabili da chiunque, senza alcun controllo, e l'impossibilità di rimuoverli definitivamente pregiudicano il diritto all'oblio e violano la legge sulla privacy.

La persona che chiede di fruire del diritto all'oblio può rivolgersi al Tribunale chiedendo un provvedimento di urgenza ingiungendo, al titolare del sito in questione, di rispettare il diritto all'oblio cancellando il nome e le foto dai contenuti pubblicati.

Se debitamente provato che il diritto all'oblio non è stato rispettato è possibile anche chiedere il risarcimento dei danni.

Per quel che riguarda il dominio che non ha rispettato il diritto all'oblio, in via penale è possibile anche il sequestro preventivo del sito, come chiarisce la sentenza del 29 gennaio 2015 della Corte di Cassazione soprattutto se il sito non sia una testata giornalistica (equiparabile alla carta stampata) poiché in quel caso godrebbe della garanzia di insequestrabilità.

Se i server del sito, invece, sono all'estero e non in Italia, il giudice non può disporre il sequestro preventivo ma può presentare domanda per l'oscuramento del sito impedendo agli utenti italiani di accedervi attraverso i provider, con tutte le difficoltà del caso documentate dai recenti

DIRITTO ALL'IMMAGINE

Il diritto all'immagine è un diritto personale avente ad oggetto il segno distintivo essenziale dell'individuo volto a rappresentarne le sembianze, l'aspetto fisico, l'espressione e, più in generale, la sua personalità.

Esso trova disciplina nel combinato disposto dell'art. 10 del codice civile e degli artt. 96 e 97 della legge 633/1941 (legge sul diritto d'autore).

Dalla normativa in esame si ricava che **il ritratto di una persona** non può essere esposto, pubblicato o messo in commercio **senza il consenso** (espresso o tacito) dell'interessato.

E' inoltre necessario che la pubblicazione/esposizione/commercializzazione non determini un pregiudizio al decoro e alla reputazione del soggetto rappresentato.

Con Facebook e la sua facilità di pubblicare e condividere immagini e filmati, si è in parte dimenticata la legislazione che regola la pubblicazione di immagini altrui (Legge del 22 aprile 1941 n. 633 Articolo 96) e la tutela della Privacy (d.lgs n. 196 del 2003).

La stessa amministrazione di **Facebook chiede espressamente** che le foto inserite nei profili siano in legale possesso di chi le pubblica, e che ritraggano essenzialmente chi le utilizza.

La legislazione italiana in materia, in particolare la legge n. 633/1941, stabilisce che per pubblicare l'immagine di una persona non famosa occorre la sua autorizzazione (art. 96 legge n. 633/1941).

La pubblicazione su Facebook della fotografia di una persona ha implicazioni anche rispetto alla riservatezza, in quanto la divulgazione di un'immagine costituisce una forma di trattamento dei dati personali lesiva del diritto alla privacy, come tutelato dal d.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) che stabilisce il principio fondamentale per cui "chiunque ha diritto alla protezione dei dati personali che lo riguardano".

Per "dato personale" s'intende, secondo l'art. 4 lettera b) del predetto decreto, qualunque informazione riguardante una "persona fisica identificata o identificabile.

A tal proposito il **Garante della privacy** ha chiarito che **le fotografie**, così come le riproduzioni di immagini (ivi comprese le videoriprese), rientrano nella nozione di dato personale (decisioni del 15 maggio 2002 e 19 febbraio del 2002).

Qualora l'immagine consenta di rilevare talune informazioni che la normativa sulla privacy inquadra nella categoria dei "dati sensibili" (art 4. comma 1, lett. d) del d.lgs. n. 196 del 2003: "i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale"), anche l'immagine avrà tale natura e pertanto sarà oggetto di più stretta tutela.

Tutto ciò comporta che, **colui che intenda pubblicare una fotografia rappresentativa di un soggetto identificabile, dovrà ottenerne il consenso scritto, ove tale fotografia riveli dati sensibili; negli altri casi il consenso potrà essere dato in forma diversa.**

Pubblicare immagini non autorizzate sui social network è trattamento illecito di dati personali.

Il reato di trattamento illecito di dati personali avvenuto attraverso la pubblicazione non autorizzata di immagini su un social network è da ritenersi integrato per il semplice fatto che utilizzare lo spazio web per postare le immagini equivale a destinarle a tutti coloro che in tempi e luoghi diversi abbiano gli strumenti tecnici e la legittimazione a connettersi in rete. In questo caso il giudice competente deve essere individuato con il criterio della residenza dell'imputato, vista l'impossibilità di ricorrere a criteri certi e univoci come quello di prima pubblicazione o di primo accesso. Questo è quanto emerge dalla sentenza del Tribunale di Firenze 5675/2015.

L'utilizzo del web integra il trattamento illecito – Il giudice analizza la fattispecie prevista dall'articolo 167 del codice della privacy che prevede la realizzazione del reato se dal fatto deriva nocumento o, indipendentemente da questo, se c'è stata diffusione o comunicazione dei dati personali. E nella fattispecie, il reato deve considerarsi perfezionato dal momento che la pubblicazione di immagini su un social network, e cioè attraverso l'utilizzo di uno spazio web, è da ritenersi sostanzialmente diretto erga omnes, poiché si rivolge potenzialmente a "tutti coloro che abbiano gli strumenti, la capacità tecnica e la legittimazione a connettersi, evidentemente in tempi e luoghi diversi tra loro"

La questione del diritto all'immagine, pertanto, assume rilievo sia da un punto di vista civilistico che penale.

L'immagine di un soggetto deve essere considerata sicuramente «dato personale», così come previsto dall'art.4 della Legge 196/2003 sulla tutela della privacy e, ai sensi dell'art.13 dello stesso codice, il titolare del trattamento dei dati ha l'obbligo d informare preventivamente l'interessato che il suo dato (immagine fotografica) potrà formare oggetto di trattamento, dando la possibilità all'interessato di esercitare in qualsiasi momento i diritti previsti dall'art.7 della L.196/2003 per ottenere:

1. l'aggiornamento;
2. la rettificazione;
3. l'integrazione;
4. la cancellazione del dato trattato.

In tutto questo interviene anche la Legge sulla **protezione del diritto d'autore** L.633/41, indicando nel consenso (art.96) la scriminante che esclude la responsabilità di colui che pubblica l'immagine fuori dai casi consentiti dalla legge e detta:

«Il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa, salve le disposizioni dell'articolo seguente .»

Non occorre il consenso se la persona è nota e neanche se è fotografata in virtù di qualche ufficio pubblico che ricopre, o per ragioni di giustizia o di polizia, oppure per scopi scientifici, didattici, culturali, oppure perché la riproduzione è legata a fatti, avvenimenti, cerimonie di pubblico interesse o che comunque si sono svolte in pubblico (art.97)

Anche nei casi di esclusione, sopra esposti è necessario, comunque il consenso dell'interessato laddove l'esposizione o la messa in commercio possa arrecare danno alla reputazione ed al decoro della persona ritratta (comma 2 - articolo 97).

Il **diritto all'immagine** è, altresì, tutelato dal **codice civile**, integrato dalle disposizioni speciali della L.633/41, che all'articolo 10 così detta:

«Qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta,o pubblicata fuori dai casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni.»

Il legislatore ha, inoltre, previsto per le violazioni più gravi circa il trattamento dei dati personali, sanzioni penali puntualmente dettate dall'art.167 "trattamento illecito di dati" del codice in materia di protezione dei dati personali, che così recita:

«Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18-19-23-124-126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

Procedendo ad una attenta analisi del dettato, appare chiaro che gli elementi costitutivi della fattispecie criminosa che devono necessariamente concorrere sono due:

1. "al fine di trarne per sé e per altri profitto oppure arrecare un danno ad altri" (elemento soggettivo).

Il termine "profitto" viene utilizzato dal legislatore al fine di abbracciare una vasta gamma di vantaggi e benefici che rivestono necessariamente carattere di natura economica-patrimoniale.

2. "se dal fatto deriva nocumento" , intendendo con detto termine una reale e tangibile lesione del bene sottoposto a tutela.

La Corte di Cassazione nel 2004 con la sentenza 26680, conferma la condanna di un uomo che aveva diffuso su Internet fotogrammi (scene di uno spogliarello) della sua ex fidanzata senza il consenso di quest'ultima.

Con riguardo al giudizio di colpevolezza, la Corte sottolinea che l'imputato non avendo accettato di buon grado la decisione della fidanzata di interrompere la loro relazione, aveva inviato numerosi messaggi telefonici

e lettere, tanto da costringere la giovane donna a cambiare in due occasioni il suo recapito telefonico. La stessa, quindi, secondo quanto valutato dalla Corte, aveva ricevuto un reale danno (nocumento) dalla condotta del suo ex fidanzato che aveva, con il suo comportamento, leso la sua tranquillità nonché la sua immagine sociale.

PRIVACY

Il tema della privacy in rete è ormai recepito nelle policy di tutti i maggiori social network, perché riguarda le stesse modalità di comunicazione e di pubblicazione di post e messaggi.

La privacy è il diritto di ciascuno di tenere riservate le informazioni personali attinenti alla propria vita privata.

Si tratta di un diritto che trova il fondamento costituzionale negli stessi diritti inviolabili dell'uomo, tra i quali il domicilio, la libertà e segretezza della corrispondenza e la libertà di manifestazione del pensiero.

Il Codice della privacy ha riconosciuto quale principio basilare quello secondo cui deve essere riconosciuto a "chiunque il diritto alla protezione dei dati personali" non solo mediante la garanzia della correttezza del trattamento dei dati ma, anche, mediante la possibilità di intervento degli interessati.

Sennonché tale principio, così come più in generale il nucleo centrale di quella normativa, ha dovuto fare i conti con l'applicazione ad un mondo, quello virtuale, che per sue proprie caratteristiche pone serie difficoltà nell'attuazione di forme di controllo.

La normativa sulla privacy, composta oltre che dal Codice anche dai vari provvedimenti e linee guida del Garante, prende in considerazione anche il comportamento delle persone sui luoghi di lavoro.

In particolare il Garante della Privacy, sin dal 2007 ha pubblicato le linee guida 1 Marzo 2007, in cui ha ricordato i doveri fondamentali del datore di lavoro: pubblicare un codice di comportamento che stabilisca le regole cui il lavoratore deve attenersi nell'uso delle risorse informatiche (quindi se sia consentito l'uso personale, in che termini, ecc); la possibilità di effettuare controlli sull'uso delle risorse informatiche; la verifica se il dipendente abbia o meno necessità dell'uso di Internet; le misure minime di sicurezza come le black list e quanto altro.

Il comportamento del dipendente infine è coperto dal rispettivo Codice che ogni amministrazione deve redigere e divulgare dandone opportuna informazione.

La giurisprudenza in materia è ancora poca. Ma ci sono dei casi in cui il Garante e il Tribunale civile si sono espressi come il caso di un dipendente licenziato per aver pubblicato su Facebook delle foto, riprese in azienda, dove erano visibili disegni coperti da segreto industriale.

O il caso del Tribunale di Livorno (GIP Trib. Livorno, 31.12.2012 n 38912) che ha condannato per diffamazione una lavoratrice licenziata che, dopo la cessazione del rapporto di lavoro, aveva pesantemente insultato il suo ex datore di lavoro tramite Facebook.

Un capitolo a parte è rappresentato dalla divulgazione di dati personali e i dati di salute.

I dati attinenti alla salute sono classificati dal codice privacy (d.lgs 30 giugno 2003, n. 196) come **dati sensibili** e la giurisprudenza li eleva a **dati sensibilissimi.**

Il trattamento dei dati personali consiste in qualsiasi operazione di raccolta, registrazione, organizzazione, conservazione, modificazione, utilizzo, comunicazione, diffusione cancellazione e deve essere trattato lecitamente e secondo correttezza, per scopi determinati, espliciti e legittimi.

Di ogni trattamento deve essere data informativa ed acquisito il consenso dell'interessato.

Il Garante privacy, nelle linee guida sull'uso del social network del maggio del 2014, ha raccomandato agli utenti:

- di valutare bene quali dati inserire nel proprio profilo;
- di evitare di fornire l'indirizzo e il numero telefonico di casa, soprattutto se minorenni;
- possibilmente, l'uso di uno pseudonimo;
- di prestare particolare attenzione alla privacy degli altri, soprattutto se si pubblicano dati personali o fotografie senza il loro consenso.

STATUTO DEI LAVORATORI

A seguito dell'entrata in vigore, il 24 settembre 2015, del decreto legislativo n. 151/2015 attuativo della legge delega n. 183/2014 ("Jobs Act"), che ha ridisegnato la disciplina relativa al controllo a distanza dei lavoratori, modificando l'articolo 4 della Legge 300/1970 ("Statuto dei Lavoratori") e adeguandolo al livello tecnologico delle strutture aziendali di oggi, occorre segnalare una rilevante novità in materia.

La norma vigente prevede **il generale divieto di utilizzare impianti audiovisivi o apparecchiature volte "esclusivamente" al controllo a distanza del lavoratore** e specifica l'eccezione a tale regola: è ammesso infatti, previo accordo con le rappresentanze sindacali o autorizzazione dell'Ispettorato del lavoro, l'utilizzo di apparecchiature dalle quali derivi "indirettamente" la possibilità di un controllo a distanza, ma installate per finalità di organizzazione e sicurezza aziendali.

Con il nuovo testo, quella che era l'eccezione diventerà la regola, infatti, il datore di lavoro avrà la "facoltà" di installare e utilizzare impianti e strumenti dai quali derivi "anche" un controllo sull'attività del lavoratore esclusivamente per *esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale*.
Resta comunque l'obbligo, in capo al datore di lavoro, di stipulare un previo accordo con le rappresentanze sindacali.

Tale disposizione non apporta una modifica tanto sensibile quanto quella prevista dal secondo comma del riscritto articolo 4 dello Statuto, che introduce la vera novità della disciplina.

Ai sensi del secondo comma, infatti, il datore di lavoro non sarà più soggetto all'obbligo del previo accordo con le rappresentanze sindacali per quanto riguarda l'utilizzo degli strumenti di cui il lavoratore si serve *per rendere la prestazione lavorativa* e *per la registrazione degli accessi e delle presenze* (tablet, smartphone, portatili, etc.).

Tale disposizione, sostanzialmente, consente al datore di lavoro di verificare le modalità di utilizzo degli strumenti ricevuti dal lavoratore, senza essere vincolato all'accordo sindacale preventivo.

Il comma di chiusura del nuovo articolo 4 disciplina l'utilizzabilità delle informazioni ottenute tramite i controlli, diretti e indiretti, per finalità connesse al rapporto di lavoro e la subordina all'obbligo in capo al datore di lavoro ad **un'adeguata informazione** – ai lavoratori – **delle modalità d'uso degli strumenti e dell'effettuazione dei controlli.**

CYBERCRIME TIPICI E FATTISPECIE PENALI

I cybercrime tipici sono:

- spamming;
- trasmissione di virus informatici;
- accesso abusivo a sistema informatico;
- phishing
- stalking, minacce e molestie
- cyber stalking
- ingiuria aggravata e diffamazione
- calunnia;

- sostituzione di persona;
- trattamento illecito di dati;
- rivelazione di segreto professionale
- rivelazione ed utilizzazione di segreti di ufficio

- **Spamming**

Il principale scopo dello spamming è la pubblicità il cui oggetto può andare dalle più comuni offerte commerciali a proposte di vendita di materiale pornografico o illegale, come software pirata e farmaci senza prescrizione medica, da discutibili progetti finanziari a veri e propri tentativi di truffa.

La tutela è accordata dal c.d. Codice della Privacy (d. lgs. 196/2003): * art. 130 c.d.p. «Comunicazioni indesiderate» che comporta l'intervento del Garante

- art. 161 c.d.p. «Omessa o inidonea informativa all'interessato» che comporta una sanzione amministrativa

- art. 167 c.d.p. «Trattamento illecito di dati» che comporta una pena detentiva che può arrivare fino a tre anni di reclusione.

- **Trasmissione di virus informatici**

Tale processo avviene con un malware che indica un qualsiasi software usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata. Il malware non necessariamente è creato per arrecare danni tangibili ad un computer o un sistema informatico, ma va inteso anche come un programma che può rubare di nascosto informazioni di vario tipo, da commerciali a private, senza essere rilevato dall'utente anche per lunghi periodi di tempo.

Il reato in Italia è configurato e punito con:

-art. 615 quinques c.p. che prevede pene detentive fino a due anni oltre pene pecuniarie.

E per

- **Accesso abusivo a sistema informatico**

- art. 615 ter c.p. che prevede pene detentive fino a tre anni salvo rivesta una posizione di garanzia.

- **Phishing** (ovvero la truffa)

  Il phishing è una minaccia attuale, il rischio è ancora maggiore nei social media come Facebook, Twitter, e Google+. Degli hacker potrebbero infatti creare un clone del sito e chiedere all'utente di inserire le sue informazioni personali. Gli hacker comunemente

traggono vantaggio dal fatto che questi siti vengono utilizzati a casa, al lavoro e nei luoghi pubblici per ottenere le informazioni personali o aziendali.

- art. 615 ter c.p. che prevede pene detentive fino a tre anni oltre pene pecuniarie.

- **Stalking, minacce e molestie** (Art. 612-bis c.p. «Atti persecutori»)

«Salvo che il fatto costituisca più grave reato, è punito con la reclusione da sei mesi a cinque anni chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini vita.»

Alla fattispecie dello «stalking» vengono ricondotte diverse altre ipotesi criminose quali la minaccia (art. 612 c.p.) e la molestia 660 c.p.).

Lo stalking è, infatti, un'estensione di queste ultime. L'elemento distintivo tra gli atti persecutori e le altre figure è la reiterazione dei comportamenti offensivi. Lo stalking è un reato abituale, a forma libera, di danno e di evento. Per la sua configurazione è infatti richiesto che le condotte cagionino, alternativamente:

- Un perdurante e grave stato di ansia
- Un fondato timore per l'incolumità propria o di un prossimo congiunto
- Una sensibile modificazione delle abitudini di vita.

- **Cyberstalking**

«Il **cyberstalking** consiste nel molestare una vittima mediante comunicazione elettronica, tramite e-mail o messaggi diretti. Un **cyberstalker** si basa sull'anonimato offerto da Internet per vessare le vittime senza essere scoperto. »

«*Integrano la condotta tipica di atti persecutori, di cui all'art. 612 bis c.p., le molestie perpetrate attraverso il reiterato invio alla persona offesa di sms, mail oppure messaggi di posta elettronica sui social network » « gli atti di molestia (…) possono concretarsi anche nella trasmissione da parte dell'indagato, tramite Facebook, di un filmato che ritraeva un rapporto sessuale tra lui e la donna* » - Cass Pen. Sez. VI n. 32404/2010

«*Integrano l'elemento materiale del delitto di atti persecutori le condotte riconducibili alle categorie del c.d. stalking vigilante (controllo sulla vita quotidiana della vittima), del c.d. stalking comunicativo (consistente in contatti per via epistolare o telefonica, Sms, scritte su muri ed altri messaggi in luoghi frequentati dalla persona offesa) e del c .d. cyber stalking, costituito dall'uso di tutte quelle tecniche di intrusione molesta nella vita della vittima rese possibili dalle moderne tecnologie*

informatiche e, segnatamente, dai social network» Trib. Termini Imerese Ordinanza del 9 febbraio 2011.

- **Ingiuria e diffamazione**

  Art. 594 c.p. «**Ingiuria**»

«Chiunque offende l'onore o il decoro di una persona presente è punito con la reclusione fino a sei mesi o con la multa fino a euro 516.»

Il reato **di ingiuria** è stato **depenalizzato** nel 2016, ma continua a costituire reato nella formulazione di **ingiuria aggravata**, cioè quando è perpetrato alla presenza di più persona, pertanto ai fini del presente scritto.

«Chiunque offende l'onore o il decoro di una persona presente è punito con la reclusione fino a sei mesi e con la multa fino a 516 euro. Alla stessa pena soggiace chi commette il fatto mediante comunicazione telegrafica o telefonica o con scritti o disegni, diretti alla persona offesa. La pena è della reclusione fino a un anno o della multa fino due milioni, se l'offesa consiste nell'attribuzione di un fatto determinato. Le pene sono aumentate qualora l'offesa sia commessa in presenza di più persone.»

Dal corollario appare chiaro perché si configuri il reato di ingiuria è necessario che l'offesa sia compiuta alla presenza del soggetto offeso e che lo stesso ne abbia l'effettiva percezione della natura offensiva della pronuncia e/o della scrittura da parte del reo (elemento soggettivo).

- Art. 595 c.p. «**Diffamazione**»

L'articolo 595 de c.p. punisce invece la **diffamazione** e così detta:

«*Chiunque, fuori dai casi indicati nell'articolo precedente comunicando con più persone, offende l'altrui reputazione è punito con la reclusione fino a u n anno o con la multa fino a due milioni. Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a quattro milioni. Se l'offesa è recata con mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a un milione.* »

(Si cita, per completezza espositiva, anche l' art. 596 bis c.p. Diffamazione col mezzo della stampa.)

«*Se il delitto di diffamazione è commesso col mezzo della stampa le disposizioni dell'articolo precedente si applicano anche al direttore o vice-direttore responsabile, all'editore e allo stampatore, per i reati preveduti negli articoli 57, 57-bis e 58.*»

Dall'analisi del testo emerge che affinché si configuri il reato di diffamazione, è necessario che si realizzi la compresenza di tre elementi costitutivi:

1. l'assenza dell'offeso

2. l'offesa deve riguardare l'altrui reputazione

3. la percezione dell'offesa da parte di più persone

In Italia una delle primissime sentenze in tema di risarcimento danni per diffamazione compiuta su social network (Facebook) è la sentenza n. 770 del 2 marzo 2010 del Tribunale Civile di Monza.

Secondo la Cassazione anche i commenti a sfondo sessuale, postati sulla bacheca della vittima, possono rientrare nel reato di molestie. Ma ad una condizione: devono essere tanto costanti e petulanti da recare disturbo nella parte offesa o costringere quest'ultima a mutare le proprie abitudini di vita.

La Corte di recente si è pronunciata sulla fattispecie analizzata con la sentenza n. 50 del 2017, ove ha chiaramente affermato che offendere attraverso i social network possa essere considerata a tutti gli effetti diffamazione aggravata.

Tale orientamento è stato rapidamente superato con la sentenza n. 4873 del 2017 della Corte di Cassazione, che ha rafforzato ancora di più la portata delle offese tramite Facebook ed ha introdotto un'altra veste al reato, come viene descritto nel paragrafo sulla calunnia.

Alcune considerazioni

Per rispondere al quesito se l'offesa sul social network configuri un reato di ingiuria o di diffamazione, occorre partire dal seguente assunto. A fare da spartiacque è la presenza della persona offesa al momento dell'azione lesiva. In dottrina, si è rilevato che, da un lato, il destinatario delle affermazioni lesive potrebbe in astratto sempre percepire direttamente l'offesa; dall'altro lato, invece, che la presenza virtuale di un soggetto è in realtà molto offuscata rispetto a quella fisica, perdendo di importanza nell'indistinta massa di utenti di una piattaforma sociale.

La giurisprudenza ha superato ogni controversia teorica applicando modelli reali al mondo virtuale.

Se l'affermazione lesiva sarà comunicata in privato (ad es. in chat) sarà integrata la fattispecie dell'ingiuria; se sarà, invece, comunicata pubblicamente, sarà integrata la diffamazione.

La diffamazione, tuttavia, sarà sempre da ritenersi aggravata ai sensi del comma 3 dell'art. 595 c.p. integrando il social network i requisiti per essere considerato "mezzo di pubblicità".

La già citata Legge 547/93, nonostante abbia previsto ed introdotto una serie di ipotesi illecite relativamente ai c.d."reati informatici", non ha previsto la possibilità della configurazione del reato di ingiurie e diffamazione perpetrato attraverso la Rete internet.

Al riguardo e a colmare tale lacuna, però, la giurisprudenza è concorde nel ritenere che le fattispecie criminose previste dagli art.594 (ingiurie) e 595 (diffamazione) del c.p., ricomprendono anche tutti quei comportamenti

lesivi dell'onore e del decoro di una persona che si realizzano attraverso le nuove forme di comunicazione nate grazie alle attuali tecnologie informatiche.

La Corte di Cassazione, con la sentenza 4741 del 2000, al riguardo stabilisce:

«Il legislatore, pur mostrando di aver preso in considerazione la esistenza di nuovi strumenti di comunicazione, telematici ed informatici, non ha ritenuto di dover mutuare o integrare la lettera della legge con riferimento a reati (e, tra questi certamente quelli contro l'onore la cui condotta consiste nella (o presuppone la) comunicazione dell'agente con terze persone. E tuttavia, che i rati previsti dagli articoli 594 e 595 c.p. possono essere commessi anche per via telematica o informatica, è addirittura intuitivo; basterebbe pensare alla cosiddetta trasmissione via e-mail, per rendersi conto che è certamente possibile che un agente, inviando a più persone messaggi atti ad offendere un soggetto, realizzi la condotta tipica del delitto di ingiuria (se il destinatario è lo stesso soggetto offeso) o di diffamazione (se i destinatari sono persone diverse)».

Quel giudice ha condannato a un giovane al risarcimento del "d*anno morale soggettivo o, comunque del danno non patrimoniale*" sofferti dalla persona offesa per la subita lesione "*della reputazione e dell'onore*" cagionata mediante l'invio di un messaggio tramite il diffuso social Network «Facebook».

- **Calunnia**

La diffamazione su Facebook è, secondo la Corte di Cassazione, «calunnia» (sentenza n. 4873 del 2017), non è considerata dalla Corte di Cassazione come diffamazione a mezzo stampa.

Con la sentenza numero 4873 del 2017 i giudici fanno notare che anche se Facebook è un mezzo capace di raggiungere e amplificare notizie, calunnie o diffamazioni, non può essere equiparato alla stampa non essendo un organo di stampa.

Anche se Facebbok ormai è diventato più persuasivo della stampa, la pena prevista dalla legge numero 47 del 1948 esclude gli organi non di stampa dimezzando per essi la pena da 6 a 3 anni .

La motivazione è attualmente la seguente "*poiché questa modalità di comunicazione di un contenuto informativo suscettibile di arrecare discredito alla reputazione altrui, ha potenzialmente la capacità di raggiungere un numero indeterminato di persone, perché attraverso questa 'piattaforma virtuale' gruppi di soggetti valorizzano il profilo del rapporto interpersonale allargato ad un numero indeterminato di aderenti al fine di una costante socializzazione (Sez. 5, n. 8328 del 13/07/2015 – dep. 01/03/2016, Martinez, non massimata sul punto), tuttavia, proprio queste peculiari dinamiche di diffusione del messaggio screditante, in una con la loro finalizzazione alla socializzazione, sono tali da suggerire l'inclusione della pubblicazione del messaggio diffamatorio sulla bacheca 'facebook' nella tipologia di "qualsiasi altro mezzo di pubblicità', che, ai fini della tipizzazione della circostanza aggravante di cui all'art. 595,*

comma 3, cod. pen., il codificatore ha giustapposto a quella del 'mezzo della stampa' (Sez. 1, n. 24431 del 28/04/2015 – dep. 08/06/2015, Conflitto di competenza, Rv. 26400701). "

Si ricorda che le Sezioni Unite avevano compreso nel concetto di testate giornalistiche online specificando che «tale operazione ermeneutica non può riguardare in blocco tutti i nuovi media, informatici e telematici di manifestazione del pensiero (forum, blog, newsletter, mailing list, e social) ma deve rimanere circoscritto a quei casi che, per i profili strutturale e finalistico, sono riconducibili al concetto di stampa: caratterizzata quest'ultima, in sostanza, dalla "professionalità" di chi scrivendo diffama».

- **Sostituzione di persona (Art. 494 c.p.)**

«*Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona , o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici , è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno*.»

La sostituzione di persona è un reato plurioffensivo: lesione della pubblica fede e vantaggio all'agente o un danno ingiusto alla persona offesa. L'elemento soggettivo è il dolo specifico : la sostituzione deve essere illegittimamente voluta e ricercata, deve concretizzarsi in atti fraudolenti. L'elemento oggettivo è l'induzione in errore che deve fondarsi su un atto commissivo.

Secondo la giurisprudenza: « *integra il reato di sostituzione di persona, la condotta di colui che crei ed utilizzi un account di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete internet, nei confronti dei quali le false generalità siano declinate e con il fine di arrecare* danno al soggetto le cui generalità siano state abusivamente spese» (Cfr. Cass. Civ. nn. 46674/2007 e 12479/2012).

E' una ipotesi illecita inserita nel capo IV, sotto il titolo VII, denominato "della falsità personale" posto a tutela della pubblica fede, contro tutti quei comportamenti legati alla identità personale e caratterizzati dall'inganno ai danni di un numero indeterminato di individui che, nell'ambito dei rapporti sociali, devono dare fiducia a determinate attestazioni.

Per la configurazione della fattispecie criminosa è richiesto il dolo specifico (elemento soggettivo), quindi la volontà del reo di indurre qualcuno in errore ed il comportamento deve essere tale da procurare a sè o ad altri un vantaggio (patrimoniale e non) o arrecare danno al soggetto a cui è stata sottratta l'identità.

E' evidente quindi che non tutte le condotte di sostituzione di persona sono perseguibili penalmente, il reato si configu

quando l' altro è tratto in errore sulla identità personale dell'autore;

- quando i comportamenti sono posti in essere con dolo specifico con lo scopo di procurare a sè o ad altri un vantaggio o di recare un danno.

Tale norma trova la sua applicazione nell'ambito delle nuove tecnologie, pur non rientrando nelle previsioni dei crimini informatici introdotte con la Legge 547 del 1993.

Puntuale risposta della giurisprudenza al riguardo, è la sentenza n.46674 del 2007 della Corte di Cassazione che ha confermato la condanna di un soggetto creatore un account di posta elettronica intestato ad un'altra persona, utilizzato per instaurare rapporti con altri utenti della Rete inducendoli, quindi, in errore.

A parere della Corte, il fatto in esame integrava gli elementi della fattispecie criminosa in esame (reato di sostituzione di persona) in considerazione del fatto che il comportamento posto in essere pregiudicava il bene tutelato dalla norma : la "fede pubblica".

«Oggetto della tutela penale, in relazione al delitto preveduto nell'art.494 c.p. è l'interesse riguardante la pubblica fede, in quanto questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali. E siccome si tratta di inganni che possono superare la ristretta cerchia di un determinato destinatario, così come il legislatore ha ravvisato in essi una costante insidia alla fede pubblica e non soltanto alla fede privata e alla tutela civilistica del diritto al nome».

- **Rivelazione di segreto professionale (Art. 622 c.p.)**

Chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa , ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto può derivare nocumento, con la reclusione fino a un anno o con la multa da trenta euro a cinquecentosedici euro.

La pena è aggravata se il fatto è commesso da amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci o liquidatori o se è commesso da chi svolge la revisione contabile della società.

Il delitto è punibile a querela della persona offesa rt. 622 c.p.

- **Rivelazione ed utilizzazione di segreti di ufficio (- Art. 326 c.p.)**

Il pubblico ufficiale o la persona incaricata di un pubblico servizio, che, violando i doveri inerenti alle funzioni o al servizio, o comunque abusando della sua qualità, rivela notizie di ufficio, le quali debbano rimanere

segrete, o ne agevola in qualsiasi modo la conoscenza, è punito con la reclusione da sei mesi a tre anni.

Se l'agevolazione è soltanto colposa, si applica la reclusione fino a un anno.

Il pubblico ufficiale o la persona incaricata di un pubblico servizio, che, per procurare a sé o ad altri un indebito profitto patrimoniale, si avvale illegittimamente di notizie di ufficio, le quali debbano rimanere segrete, è punito con la reclusione da due a cinque anni. Se il fatto è commesso al fine di procurare a sé o ad altri un ingiusto profitto non patrimoniale o di cagionare ad altri un danno ingiusto, si applica la pena della reclusione fino a due anni.

- **postare immagini altrui (a metà strada fra civile e penale** violazione del diritto alla privacy, del diritto d'autore e del diritto all'immagine)

TIPOLOGIE DI SOCIAL NETWORK E PRINCIPALI CARATTERISTICHE

Alcune tra le più conosciute Piattaforme disponibili sul web sono:

Tipologia	Funzioni	Esempi	Uso comune
Blog (da web-log, sito web i cui contenuti vengono visualizzati in forma anticronologica; generalmente gestito da un blogger che gestisce gli interventi)	Consente agli utilizzatori di generare e postare i propri contenuti	Pagina personale Blog di attualità/informazioni Blog tematico Blog vetrina Blog aziendale	Per scrivere sui propri interessi Generare dibattiti Scambiarsi conoscenze tra esperti Attrarre nuovi clienti
Social Networking Site	Consente di creare un profilo personale, di connettersi con altre persone, scambiare messaggi e realizzare gruppi di scambio di interessi, con la possibilità di collegamento a siti	Facebook MyPsace Google+	Sono network che prevedono preselezione di amici e conoscenti Permettono scambio di informazioni personali, immagini, eventi, filmati etc Messaggi Pagine per il business
Short Networking/ blog	Sono network e blog che consentono di comunicare con chiunque e scambiare informazioni attraverso messaggi molto brevi	Twitter (i messaggi sono chiamati tweet e possono essere lunghi fino a 140 caratteri	post personali o relativi alla propria attività Post relativi alle proprie opinioni o pensieri Per gli approfondimenti si rinvia ad un sito o ad altro contenuto web
Piattaforme di Media sharing	Permette di vedere o scambiarsi video	YouTube	Scambio di video

	rispetto ad una platea globale		Scambio di informazioni legate al marketing Post relativi a interviste, corsi, etc
Podcast	Permettono di scaricarsi files generalmente audio o video	Varie piattaforme	Piccoli video Interviste Materiali di marketing etc
Business Networking site	Permettono ai professionisti di scambiarsi informazioni e messaggi e sono il campo di incontro tra domanda e offerta	LinkedIn	Scambio di informazioni professionali finalizzate all'impiego
Text	Permettono di scambiarsi testi e messaggi (sms, whatsapp)	Varie piattaforme generalmente collegate al sistema della fonia fissa o mobile	Generalmente sono usati per le comunicazioni interpersonali o di piccoli gruppi e si sta ampliando l'uso per lavoro
Wiki	Sito che consente a chi ne decide l'uso di aggiungere, modificare e cancellare testi tematici di uso comune (web)	Sono basati su un software come il MediaWiki (esempio wikipedia)	E' una comunità di contenuti che gestisce la conoscenza inserendo definizioni, documenti, note rispetto ad un determinando argomento

NORMATIVA – SENTENZE E BIBLIOGRAFIA

Bibliografia

Federazione Nazionale Infermieri 2013 http://www.ipasvi.it/attualita/gli-infermieri-sui-social-media-usarli-correttamente-un-opportunit-id1109.htm

American Nurses Association (ANA) (2011) ANA's Principles for Social Networking and the Nurse. American Nurses Association, http://www.nursesbooks.org

HIMSS Europe, Socila media in Healthcare: privacy and security consideration by the HIMSS Privacy and Security Committee, 2012

KAISER PERMANENTE, Social Media Policy, september 2011

The National Academies Press, Public response to alert and warning using social medita, Privacy and legal challenges with the use of social media, 2013

ECDC, Social media strategy development, a guide to using media for public health communication, 2016

European Journal for Public Helath, Social media for public helath: an exploratory policy analysis, vol 25, No.1, 162-166, June 2014

NHS Employers, quick guide for new starters, to using social media in the NHS, november 2014

Social media and health care professionals: benefits, risks and best practices, in P&T vol 39, No.7, July 2014

Sentenze

Corte di Giustizia Europea Sez. III 360 del 16 febbraio 2012

Tribunale di Genova sez. I, sentenza del 13 luglio 2012, n. 3443

Corte Cassazione Civile, sez. III, sentenza 26 giugno 2013 n. 16111

Corte di cassazione Sezioni unite penali sentenza 29 gennaio 2015, n. 31022

Tribunale di Firenze Sez. II Penale sentenza 8 gennaio 2015, n. 5675

Corte di Cassazione Sez. III Penale sentenza 1 luglio 2004 n. 26680

Le linee guida del Garante per posta elettronica e internet (Gazzetta Ufficiale n. 58 del 10 marzo 2007)

GIP Trib. Livorno, 31 dicembre 2012 n 38912

Social privacy. Come tutelarsi nell'era dei social network
(http://194.242.234.211/documents/10160/2416443/Social+privacy.
+Come+tutelarsi+nell'era+dei+social+network.pdf

Corte Cassazione Penale Sez. VI sentenza 16 luglio - 30 agosto 2010, n. 32404,

Trib. Termini Imerese Ordinanza del 9 febbraio 2011

Normativa nazionale

Legge 9.01.2004 n. 4 "Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici" e successivi decreti attuativi;

Direttiva 24.10.2005 del Ministro per la funzione pubblica sulla semplificazione del linguaggio delle pubbliche amministrazioni;

Direttiva 18 novembre 2005 del Ministro per l'innovazione e tecnologie sulle linee guida per la pubblica amministrazione digitale;

D.lgs. 82/2005 Codice dell'amministrazione digitale e smi;

Linee guida per la comunicazione on line del Ministero della Salute, dicembre 2010;

Vademecum pubblica amministrazione e social media 2012

Linee guida del garante della privacy in materia di trattamento dei dati personali contenuti anche in atti e documenti amministrativi emanati da soggetti pubblici per finalità di pubblicazione diffusione sul Web, pubblicati sulla Gazzetta Ufficiale N. 64 del 19/03/2011;

Decreto legislativo 30 giugno 2003, n. 196 (Codice privacy)

Codice penale

Codice civile

Legge 22 aprile 1941, n. 633 e sue m.i