Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Base legale per i media sociali

Rapporto del Consiglio federale in adempimento del postulato Amherd 11.3912 del 29 settembre 2011

Compendio

I media sociali (o reti sociali) sono piattaforme più o meno aperte, interattive e partecipative che consentono ai loro utenti di comunicare tra loro nonché di stringere e coltivare rapporti. Compiendo uno sforzo minimo, gli utenti hanno la possibilità, individualmente o collettivamente, di produrre contenuti, di rendere questi ultimi accessibili ad altri utenti o di scambiarli con o mediante terzi. A fronte di questo contesto appaiono labili i confini tra autore, produttore, divulgatore e utente, tra comunicazione privata e comunicazione pubblica. I media sociali si finanziano principalmente attraverso la vendita dei dati dei loro utenti a imprese, che li usano a fini pubblicitari.

In risposta alla domanda posta dalla consigliera nazionale Amherd in merito all'attuale quadro giuridico disciplinante i media sociali, il presente rapporto illustra gli standard e le raccomandazioni internazionali, esaminando in tale contesto le disposizioni svizzere vigenti. Nel rapporto si giunge alla conclusione che in materia di media sociali non sussiste al momento la necessità di un disciplinamento specifico simile a quello adottato in ambito radiotelevisivo. La molteplicità delle opportunità e dei rischi legati ai nuovi canali di comunicazione produce un quadro generale ricco di sfaccettature. L'esperienza acquisita finora mostra che la legislazione svizzera non presenta lacune gravi. Applicate con giudizio, le disposizioni formulate in modo generale nelle leggi in vigore (ad es. LPD, CP, CC, LCSI) forniscono una risposta appropriata alla maggior parte dei problemi che le piattaforme sociali pongono o potrebbero porre ai singoli individui e all'intera collettività.

Non si può tuttavia garantire che le disposizioni esistenti si riveleranno efficaci nella pratica. Ciò vale specialmente per l'applicazione del diritto in caso di controversia, che potrebbe risultare precaria a causa dell'orientamento internazionale delle piattaforme, dell'anonimità dei contenuti diffusi e della difficoltà di ascrivere la responsabilità ai diversi soggetti coinvolti (utenti, gestori delle piattaforme, fornitori di servizi Internet, ecc.). Il carattere transfrontaliero di questo fenomeno riduce in molte circostanze il margine di manovra di cui dispone il legislatore svizzero. In alcuni ambiti, non si esclude tuttavia la possibilità che alcune modifiche di legge possano contribuire a migliorare la situazione, ad esempio in materia di protezione dei dati, di protezione della gioventù dai rischi dei media e di riconoscimento della responsabilità dei fornitori di servizi che permettono l'accesso a una rete (gestori di piattaforme e fornitori di servizi Internet).

Molte di queste questioni sono attualmente sottoposte ad analisi approfondite, le quali concernono altresì la comunicazione sulle piattaforme sociali. I lavori di revisione della legge sulla protezione dei dati apporteranno maggiore chiarezza sull'eventuale necessità di legiferare anche in materia di media sociali. In tema di protezione della gioventù, l'efficacia dei provvedimenti esistenti saranno esaminati nel quadro del programma nazionale «Gioventù e media».

Oltre a ciò, s'impone sempre più l'urgenza di esaminare nel dettaglio la necessità di introdurre delle disposizioni specifiche che definiscano la responsabilità giuridica dei gestori delle piattaforme e dei fornitori di servizi Internet. Se questa analisi evidenzierà la necessità di una modifica di legge, sarà posto in consultazione un progetto in tal senso.

L'inclusione dei media sociali nell'ambito della legislazione sulle telecomunicazioni sarà pertanto chiarita nel quadro del progetto di consultazione concernente la revisione della legge sulle telecomunicazioni. Secondo la pianificazione attuale, la revisione della LTC sarà commissionata dal Consiglio federale nel corso della presente legislatura.

Come precedentemente esposto, le diverse attività e analisi non vertono unicamente sui media sociali, ma sono da considerarsi in relazione all'intero sistema giuridico. Ad ogni modo, anche i diversi aspetti relativi ai media sociali devono essere nell'insieme coerenti sul piano contenutistico. Dovrà essere pertanto garantita la circolazione delle informazioni tra i servizi coinvolti. In ultimo, sarebbe inoltre auspicabile tracciare nuovamente il punto della situazione del quadro giuridico disciplinante i media sociali, non appena saranno conclusi i suddetti lavori e sarà meglio definito l'orientamento da seguire.

Indice

1 Introduzione: postulato Amherd 11.3912

Nel suo postulato del 29 settembre 2011[1], la consigliera nazionale Viola Amherd segnala che, i media sociali aprono una nuova dimensione nel campo della comunicazione e dell'utilizzo dei media che minaccia di pregiudicare l'applicazione delle leggi nazionali e dei diritti fondamentali. Si pensi soprattutto alle disposizioni in materia di protezione dei dati, alla lotta contro il razzismo o, più in generale, alla protezione della sfera privata. È pertanto possibile che occorra porvi rimedio con un'apposita regolamentazione per i media sociali.

L'autrice del postulato chiede al Consiglio federale di stilare un rapporto sullo stato attuale della legislazione sui media sociali, nel quale risponderà in particolare alle seguenti domande:

- Come si presenta la legislazione attuale, in Svizzera e all'estero, relativa ai media sociali?
- Quali aspetti presentano delle lacune?
- Come possono essere colmate?
- Cosa pensa il Consiglio federale dell'elaborazione di una legge consacrata ai media sociali, che consideri le peculiarità di queste nuove piattaforme di comunicazione?

Nella sua presa di posizione del 23 novembre 2011, il Consiglio federale si chiede se il diritto vigente (soprattutto nella LPD, nel CC, nel CP e nella LDA) sia in grado di affrontare opportunamente i problemi e chiarire le responsabilità dei soggetti coinvolti. Problemi specifici si riscontrano ad esempio nell'ambito della tutela degli utenti dall'abuso dei propri dati personali; vi sono inoltre molte lacune nei sistemi di trasferimento di dati dall'una all'altra piattaforma di media sociali. Un'altra problematica centrale in relazione ai media sociali riguarda anche l'applicazione della legge in vigore: essendo i gestori di piattaforme di media sociali spesso attivi a livello internazionale, la legislazione nazionale mostra tutti i suoi limiti. Il Consiglio federale propone di accogliere il postulato.

Il presente rapporto è stato redatto sotto la guida dell'Ufficio federale delle comunicazioni. I lavori sono stati condotti in accordo con l'Ufficio federale di giustizia, il Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI), l'Ufficio federale delle assicurazioni sociali e l'Ufficio federale della sanità pubblica, nonché un gruppo di esperti incaricati della revisione della legge federale sulla protezione dei dati. Il rapporto è stato completato dalle opinioni di tre esperti (sulle questioni terminologiche nel campo dei social media, sull'applicazione del diritto nel contesto internazionale e sulla violazione dei diritti dei privati).

[1] http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20113912

2 Media sociali (reti sociali)

2.1 Termini

L'espansione di Internet a banda larga avvenuta negli scorsi anni ha dato un'enorme spinta ai media sociali (reti sociali)[2]. Anche in Svizzera si assiste a una fruizione intensa di questi media. Il 47 per cento degli svizzeri accedono a comunità online o reti sociali online private, il 22 per cento fa capo a reti sociali online professionali e l'11 per cento al servizio di microblogging Twitter[3]. Due terzi delle imprese, autorità e organizzazioni svizzere curano attivamente la loro presenza sui media sociali, solo il 34 per cento non è presente sul web sociale[4]. Le reti sociali sono generalmente piattaforme più o meno aperte, interattive e partecipative che permettono agli utenti di comunicare, costruire e intrattenere relazioni. Inoltre, con uno sforzo minimo, gli utenti dei media sociali possono scambiare informazioni e contenuti di e su terzi oltre che generare contenuti, sia personalmente che in cooperazione con altri, per poi renderli accessibili ad altri utenti. In Svizzera oltre un milione di persone produce e diffonde in Internet contenuti propri; caricare foto e immagini in movimento in Internet figura tra le attività più popolari[5].

I media sociali assumono forme sempre più diverse. A seconda dell'architettura della piattaforma ideata dai gestori e delle possibilità di in interagire con altre piattaforme, offrono varie possibilità di utilizzo, interazione e sviluppo della piattaforma stessa.

Spesso i media sociali permettono di instaurare rapporti di collaborazione spontanei tra utenti che ritengono rilevanti i contenuti di altri, li riprendono, migliorano, rielaborano e collocano in un nuovo contesto. Così facendo si creano nuove opere comuni, senza che siano state previste in precedenza[6].

Per la maggior parte degli utenti, i media sociali servono prevalentemente per scambiarsi messaggi privati all'interno di una cerchia ristretta di persone che si conosce. Parallelamente queste reti vengono spesso utilizzate anche per messaggi pubblicitari professionali volti a influenzare il comportamento d'acquisto dei consumatori o la formazione dell'opinione pubblica.

Le reti sociali si caratterizzano viepiù dalle possibilità di spostare le frontiere, che rispetto ai classici canali di comunicazione e media, sono incentrati in particolare su tre ambiti:

2.1.1 Frontiere permeabili tra autore, produttore, divulgatore e utente

Mentre nei media tradizionali vi è spesso una chiara separazione tra chi fornisce le prestazioni (ad es. redattori professionisti, registi, case editrici) e chi ne fruisce (pubblico); i membri di una rete sociale possono facilmente assumersi entrambi i ruoli, quello di produttori e di consumatori. I profani possono creare contenuti singolarmente o in gruppo oppure modificare contenuti creati da terzi e decidere se condividerli con altri utenti.

2.1.2 Frontiere permeabili tra comunicazione privata e pubblica

Tradizionalmente la comunicazione privata e quella pubblica passano attraverso canali distinti: nella comunicazione privata il mittente generalmente conosce il destinatario o i destinatari (si pensi alle discussioni private, lo scambio epistolare o le conversazioni telefoniche), mentre in quella pubblica il mittente non sa esattamente a chi si rivolge.

---

[2] In questo rapporto i due termini sono impiegati come sinonimi.

[3] Latzer M./Just N./Metreveli S./Saurwein F. (2012). *Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project – Switzerland 2011*. Università di Zurigo, Zurigo, pagg. 16, 19.

[4] Bernet ZHAW *Studie Social Media Schweiz* 2012, pag. 3 segg.: http://www.bernet.ch/socialmediastudie .

[5] Latzer M./Just N./Metreveli S./Saurwein F. (2012). *Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project – Switzerland 2011*. Università di Zurigo, Zurigo, pag. 17 seg.

[6] Aguiton C./Cardon D., pag. 52.

Molte offerte di media sociali permettono agli utenti un passaggio semplice tra comunicazione privata e pubblica sulla stessa piattaforma. Questo aspetto viene accentuato dal fatto che nelle reti sociali sono presenti anche i tradizionali mass-media che, se riprendono e diffondono contenuti e attività degli utenti, possono innalzare questi ultimi allo statuto di mass-media.

2.1.3 Frontiere permeabili tra trattamento dati locale e remoto

I media sociali evitano agli utenti di dover salvare dati e contenuti in uno specifico luogo fisico: collocandoli nelle reti sociali questi saranno disponibili per gli utenti ovunque essi avranno accesso alla rete in questione. La memorizzazione di contenuti su server di terzi permette un'elevata flessibilità ed efficienza nell'utilizzo ma, rovescio della medaglia: implica anche una certa perdita di controllo per quanto riguarda dati e contenuti riferiti a persone.

2.2 Categorizzazione dei media sociali

Le piattaforme sono numerose, complesse, dalle svariate funzioni e in continua evoluzione, condizioni, queste, che rendono quasi impossibile effettuare una chiara suddivisione in categorie. I media sociali sono inoltre difficilmente catalogabili poiché non rappresentano né un'evoluzione dei tradizionali mass-media, né un mezzo di comunicazione per la comunicazione puramente individuale[7]. Spesso i media sociali vengono categorizzati secondo i seguenti criteri:

2.2.1 Funzioni

Anche se spesso presentano svariate funzioni, nell'ambito della ricerca sono previste diverse categorizzazioni che distinguono almeno tra le funzioni orientate al contenuto e quelle orientate ai rapporti.

2.2.1.1 Funzioni orientate al contenuto

- Gestione dell'informazione e del sapere:
  creare, trovare, recepire, gestire e scambiare opinioni, sapere e informazioni, ad es. wiki, social bookmarking, tagging, RSS, blogosfere o piattaforme legate a interessi particolari[8].

- Intrattenimento o esperienze in mondi virtuali:
  scambio di contenuti con l'obiettivo di intrattenersi o vivere situazioni virtuali, ad es. YouTube, certi giochi interattivi online, ecc.

2.2.1.2 Funzioni orientate alle relazioni:

- Cura delle relazioni: coltivare relazioni esistenti o allacciare nuovi contatti (ad es. su piattaforme di contatto), scambio e contatto con persone dagli interessi analoghi, ad es. piattaforme relative a un determinato interesse come myspace per gli appassionati di musica.

- Gestione dell'identità e della reputazione: presentazione (selettiva) di aspetti della propria persona, ad es. in blog o podcast personali.

2.2.2 Possibilità di partecipazione

Un'altra opportunità di categorizzazione può essere data dalle opportunità tecniche a interagire sulle reti sociali. Da un lato viene valutato il grado di interazione sui contenuti scambiati, che spazia dalla semplice possibilità di valutare o commentare un contenuto fino alla creazione o alla modifica di contenuti. D'altro, invece, viene preso in considerazione anche il grado di notorietà della comunicazione, su una scala che va dalla comunicazione puramente individuale a quella di massa.

---

[7] Neuberger, Christoph, «Soziale Netzwerke im Internet. Kommunikationswissenschaftliche Einordnung und Forschungsüberblick». In. Neuberger, Christoph; Gehrau, Volker (Hrsg): *StudiVZ. Diffusion, Nutzung und Wirkung eines sozialen Netzwerks im Internet*. Wiesbaden 2011, pag. 34.

[8] Schmidt, Jan, «Was ist neu am Social Web? Soziologische und kommunikationswissenschaftliche Grundlagen». In: Zerfass, e altri editori: *Kommunikation, Partizipation und Wirkungen im Social Web*. Vol. 1. Colonia 2008, pag. 71.

2.2.3 Modelli di finanziamento

Le reti sociali non sottostanno alla legge della scarsità, funzionano infatti in modo diametralmente opposto: il valore di un prodotto o di un servizio aumenta con il numero dei fruitori. Si parla in questo caso di effetti di rete[9]. Sulle reti sociali si creano effetti di rete per svariati attori: più aumenta il numero di membri, più per tutti gli utenti cresce la possibilità di trovare sulla piattaforma persone che condividono la propria opinione, più i programmatori sono motivati a ideare applicazioni per tale piattaforma e per le agenzie pubblicitarie aumenta la probabilità di potersi rivolgere, tramite la piattaforma, a gruppi target circoscritti. Per questi motivi, le reti sociali puntano dapprima su una strategia che consente loro di attirare rapidamente molti utenti, senza generare grandi introiti. Cercano di creare un legame con gli utenti nel tentativo di evitare che si rivolgano ad altre piattaforme.

Gli effetti di scala a livello di reti e forum creano incentivi all'acquisizione e alla fusione con altri media, per poter operare nel modo più redditizio possibile. Questa situazione può, perlomeno per un tempo limitato, innalzare alcune imprese in posizione dominante.

I modelli di finanziamento dei media sociali possono essere suddivisi in forme non commerciali e forme commerciali. Dagli albori di Internet è consuetudine fruire di contenuti a titolo gratuito. Anche oggi molti media sociali non hanno fini commerciali ma sono legati all'idea della *community*. Spesso gli utenti vedono queste reti come un'opera comunitaria alla quale devono una certa lealtà, e sono quindi disposti a finanziarne la manutenzione tramite donazioni. Un'altra forma di finanziamento non commerciale dei media sociali avviene tramite fondi pubblici, dal momento che può essere nell'interesse pubblico allestire reti sociali appositamente concepite per determinati gruppi target, quali ad esempio bambini e giovani.

Tra i modelli di finanziamento commerciali dei media sociali citiamo in particolare il finanziamento attraverso le tasse d'utilizzo e la pubblicità. La pubblicità consiste prevalentemente in annunci pubblicitari adeguati in modo dinamico ai rispettivi contenuti visualizzati sullo schermo, allo scopo di attirare l'attenzione degli utenti. In minor misura si utilizza la pubblicità statica. Siccome gli utenti delle reti sociali allestiscono un proprio profilo contenente dati riguardo alla loro persona, è disponibile un numero relativamente elevato di informazioni che sono vendute a determinate aziende a scopi pubblicitari. L'allestimento di profili consente di rivolgersi a uno specifico gruppo target. Il conteggio viene fatto per ogni 1000 visualizzazioni della pubblicità o secondo il procedimento del *Cost per Click*, in cui l'agenzia pubblicitaria retribuisce la piattaforma solo se le persone interpellate hanno cliccato sul suo annuncio. I gruppi target di piattaforme specializzate[10] vengono quotati a un prezzo maggiore. Gli utenti "pagano" dunque con i propri dati personali, l'utilizzo gratuito delle prestazioni che i media sociali mettono loro a disposizione

2.3 Ruoli in relazione alla fruizione delle reti sociali

Le reti sociali coinvolgono molte parti, ognuna con un ruolo diverso. Nella prassi, però, i ruoli non sono sempre chiaramente distinguibili l'uno dall'altro, le frontiere tra le varie funzioni sono spesso permeabili.[11] I gestori di piattaforme possono infatti fungere anche da fornitori di servizi di hosting.

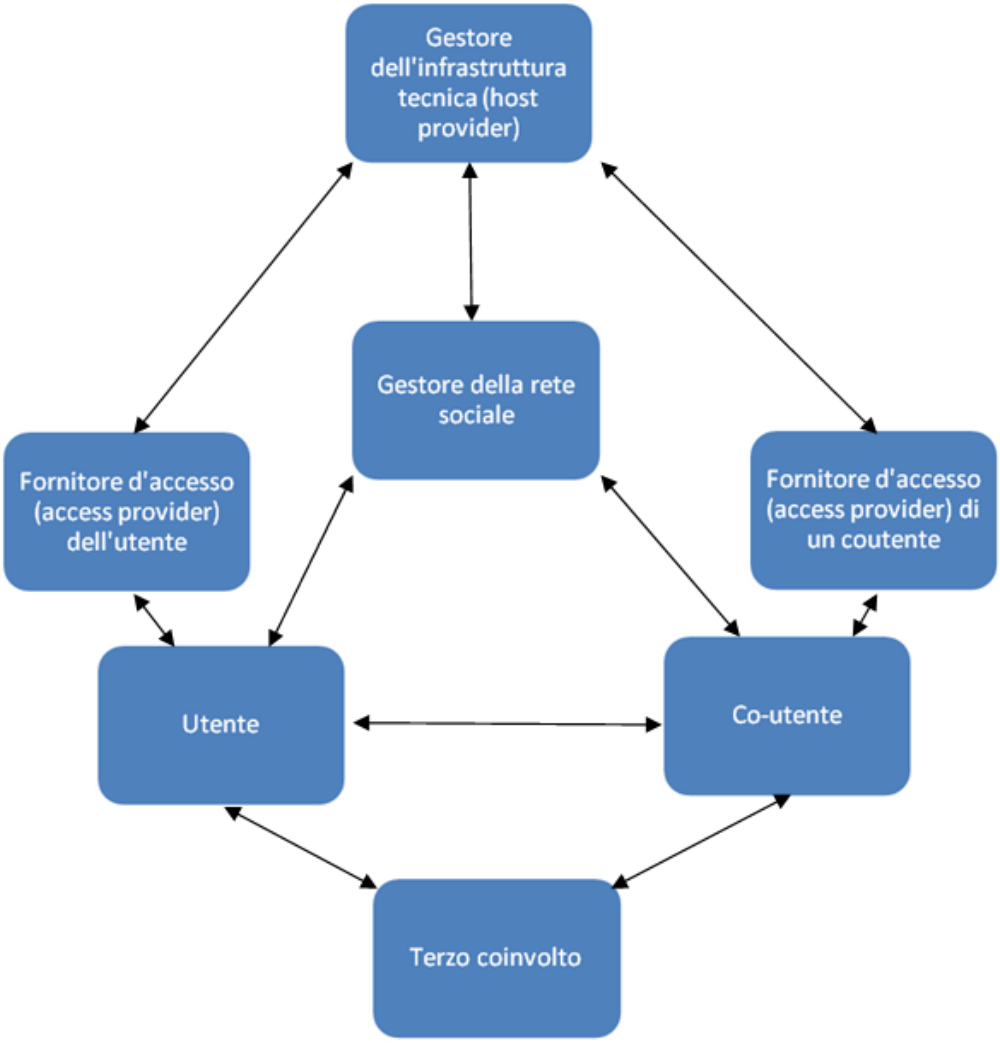
---

[9] Von Rimscha M. Björn, «Geschäftsmodelle für Social Media» in: Grimm, Petra; Zöllner, Oliver (ed.): *Schöne neue Kommunikationswelt oder Ende der Privatheit?* Stoccarda 2012, pag. 303 seg.

[10] Ad es. piattaforme orientate al mondo del lavoro come Xing o LinkedIn.

[11] Cfr. le spiegazioni relative alle varie parti coinvolte nella comunicazione in Internet nell'ambito della commissione di esperti «Criminalità in rete», DFGP 2003, pag. 27 segg.

Una prima panoramica semplificata può comunque essere rappresentata in questo modo:



2.3.1 Gestore di piattaforme di media sociali (gestore di piattaforme)

I gestori di piattaforme mettono a disposizione degli utenti un quadro per lo scambio di contenuti creati autonomamente o ripresi. Molte delle piattaforme più utilizzate in Svizzera hanno sede all'estero, tra le più popolari citiamo Facebook, YouTube e Twitter. Vi sono tuttavia anche gestori di piattaforme con sede in Svizzera. Si pensi a coloro che propongono blog che talvolta possono venir convenuti in giudizio davanti a un tribunale svizzero (ad es. la SSR[12] o determinate case editrici di giornali[13]).

Attraverso l'architettura e il design della piattaforma i gestori stabiliscono le possibilità di interazione e di diffusione dei contenuti. Decidono inoltre in che misura gli utenti possono creare spazi di comunicazione privati, semi-pubblici o pubblici e scambiare contenuti tra questi. Con l'ausilio di "Content-Rankings" e rimandi (link) a temi di terzi i gestori possono attirare l'attenzione degli utenti su determinati contenuti. Infine i gestori determinano quali dati rilevare presso gli utenti, quali diritti esercitare sui dati e i contenuti scambiati e come sfruttarli dal punto di vista economico.

---

[12] Cfr. il conflitto concernente un commento infamante nel blog relativo alla trasmissione televisiva *Alpenfestung* (DTF 136 IV 145).

[13] Cfr. il conflitto concernente il contributo lesivo della personalità pubblicato da un politico su una piattaforma di blog della Tribune de Genève (TF 5A_792/2011 del 14.1.2013).

La maggior parte dei gestori di piattaforme stabilisce regole che disciplinano il comportamento tra utenti o con terzi nonché la produzione, l'utilizzo o la diffusione di contenuti. Attraverso le condizioni d'utilizzo i gestori possono prescrivere quali sono i contenuti o i comportamenti indesiderati o vietati. Rispetto ai media tradizionali, esercitano però un controllo redazionale più blando. Mentre nei media tradizionali i contenuti sono generalmente selezionati dalla redazione prima di essere pubblicati (ex-ante), nelle reti sociali spesso il controllo viene fatto ex-post, cosicché i contenuti in contraddizione con le condizioni d'utilizzo o che sono stati criticati da altri utenti vengono rimossi in seguito (notice-and-take-down). Talune piattaforme affidano agli utenti la definizione di queste regole e rinviano alla responsabilità e alla capacità organizzativa di ognuno.

2.3.2 Fornitori di servizi Internet (servizi di hosting e di accesso)

La comunicazione tramite le reti sociali dipende da un'infrastruttura tecnica. Alcuni gestori di piattaforme memorizzano i dati su server propri. Molti altri, invece, si avvalgono dei servizi di terzi che, dietro pagamento, mettono loro a disposizione l'infrastruttura tecnica (spazio di memoria, memoria di calcolo, capacità di trasmissione) per l'attivazione automatica di dati (spesso si tratta di fornitori di servizi di hosting). La maggior parte dei gestori di piattaforme e dei fornitori di servizi di hosting presenti sul mercato svizzero ha sede all'estero. Generalmente non si assumono una propria responsabilità redazionale ma sono, a seconda della costellazione[14], tecnicamente in grado di *rimuovere* contenuti indesiderati memorizzati sui loro computer.

Il collegamento tra i pc di coloro che accedono ai media sociali e i server contenenti il materiale dati delle piattaforme viene allestito da fornitori di prestazioni d'accesso (**access-provider**), che hanno stipulato un contratto con i gestori delle piattaforme. Gli utenti svizzeri fanno generalmente capo ai servizi di fornitori di accesso con sede in Svizzera, tra i principali citiamo Swisscom. I fornitori d'accesso non sono in grado di rimuovere contenuti indesiderati poiché i dati non sono memorizzati sui loro server bensì su quelli dei fornitori di servizi di hosting. Potrebbero però, bloccare in modo mirato l'accesso a determinati contenuti (*bloccaggio*).

2.3.3 Utenti e co-utenti

In linea di massima sono gli utenti che creano contenuti (user generated content) o rinviano a contenuti di altri. A tale scopo necessitano sia del sostegno tecnico da parte dei fornitori di accesso sia dell'accesso alla rispettiva piattaforma di media sociali. In generale gli utenti possono decidere a chi rivolgersi, ossia se condividere i propri contenuti con un vasto pubblico o soltanto con una cerchia ristretta di persone. Si muovono nel quadro delle possibilità tecniche e contenutistiche predisposte dal gestore della piattaforma.

Nei confronti del gestore, gli utenti delle reti sociali hanno una (co)responsabilità riguardo al modo in cui comunicano tra loro e ai contenuti che rendono accessibili a una cerchia più ampia. Spesso, per le attività che violano basi giuridiche o i diritti di terzi, la responsabilità non è chiaramente definita o gli utenti non ne sono a conoscenza. Ciò può comportare rischi per entrambe le parti.

2.3.4 Terzi coinvolti

Le attività nei media sociali possono ripercuotersi anche su terzi che non sono attivi nelle reti in questione. Ad esempio, se contenuti che concernono terzi escono dai social media per finire nei mass media o se alcuni utenti utilizzano dati di terzi nei media sociali senza chiederne l'autorizzazione.

2.3.5 (Mass) media tradizionali e di altro tipo

I media sociali possono avvalersi dei media tradizionali per acquisire nuovi membri e per incassare maggiori introiti pubblicitari. I media tradizionali, a loro volta, attingono sempre più contenuti e novità ai media sociali.

---

[14] In alcuni casi il fornitore di servizi di hosting non può rimuovere singoli contenuti dal server dato in affitto, bensì soltanto interrompere la corrente o staccare fisicamente i dischi duri, intervento che spesso risulta essere sproporzionato.

Queste interazioni fanno sì che spesso gli utenti dei media sociali faticano a distinguere i confini tra comunicazione privata e pubblica. Molti media tradizionali hanno una propria presenza nei social media o sono collegati (ad es. tramite un link) con grandi reti sociali come Facebook.

Altri "anelli di congiunzione" possono essere i motori di ricerca che rinviano gli utenti a contenuti presenti nei media tradizionali ma anche nelle reti sociali. Si creano anche cooperazioni di tipo economico, soprattutto in relazione allo scambio e alla valutazione di dati degli utenti a scopo pubblicitario.

2.4 Osservazioni preliminari sul coinvolgimento legale dei partecipanti ai media sociali

2.4.1 Diritti e doveri derivanti dalla Costituzione

In Svizzera (e a quanto pare anche all'estero) la comunicazione tramite le reti sociali non soggiace finora a regole specifiche. Tuttavia, l'utilizzo dei media sociali non avviene in un vuoto giuridico.

A tutte le parti coinvolte (utenti, gestori di piattaforme e fornitori) l'ordinamento giuridico garantisce al massimo livello normativo la tutela dagli interventi statali. Infatti, la Costituzione svizzera e la Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali assicura la libera comunicazione (art. 16, 17, 21, 22, 23, 34 Cost. nonché art. 10 e 11 CEDU) e la libertà economica (art. 27 Cost.). Le libertà garantite attraverso questi diritti fondamentali non sono assolute ma possono essere limitate dallo Stato, nel rispetto di condizioni severe da parte delle autorità. Conformemente all'articolo 36 della Costituzione, le restrizioni dei diritti fondamentali devono avere una base legale, essere giustificate da un interesse pubblico o dalla protezione di diritti fondamentali altrui ed essere proporzionate allo scopo. Sono invece assolutamente vietati gli interventi nel tenore principale dei diritti fondamentali, come ad esempio la censura sistematica dei contenuti da parte dello Stato (art. 17 cpv. 2 Cost.).

In relazione alla comunicazione dei privati via media sociali, lo Stato è vincolato da due impegni: da un lato egli stesso non è autorizzato a violare i diritti fondamentali, dall'altro deve tutelare i diritti dei privati nei confronti di limitazioni illecite da parte di altri privati.

Oltre ad offrire opportunità, l'utilizzo delle reti sociali implica anche rischi per i diritti, sia dei singoli che della comunità. A tutela dei diritti fondamentali di terzi, o degli interessi pubblici (sicurezza o salute pubblica)[15], lo Stato deve intraprendere determinati provvedimenti giuridici come ad esempio predisporre strumenti per la protezione della sfera privata (art. 13 Cost., art. 8 CEDU). Si pensi alle disposizioni per la tutela da propositi lesivi dell'onore e diffamatori.

Bambini e giovani meritano una protezione particolare. Conformemente alla Convenzione ONU sui diritti del fanciullo gli Stati proteggono il fanciullo contro ogni forma di sfruttamento pregiudizievole al suo benessere in ogni suo aspetto (art. 36) e gli garantiscono protezione contro affronti illegali al suo onore e alla sua reputazione (art. 16)[16]. La Corte europea dei diritti dell'uomo (Corte EDU) pretende dallo Stato che intraprenda misure efficaci qualora, attraverso pubblicazioni immorali e scabrose venga arrecato pregiudizio alla vita privata di un giovane[17].

Anche la libertà dei media comporta oneri per lo Stato cui spetta adottare provvedimenti atti a contrastare la capacità di potenti attori (economici) privati di influenzare il pubblico.

---

[15] Si pensi ai provvedimento contro la pubblicità per l'alcool e il tabacco, o contro l'abuso di stupefacenti.

[16] Convenzione sui diritti del fanciullo, conclusa a New York il 20 novembre 1989, entrata in vigore per la Svizzera il 26 marzo 1997 (Convenzione sui diritti del fanciullo), RS **0.107**

[17] Sentenza della Corte EDU «K.U. c. Finlandia» (n. 2872/02) del 2.12.2008 in cui la giustizia finlandese si è rifiutata a torto di obbligare il provider a consegnare i dati sospetti.

2.4.2 Diritti e doveri nella legislazione vigente

2.4.2.1 Rispetto delle disposizioni legali generali

Le disposizioni legali stabilite dalla Costituzione sono concretizzate a livello legislativo. La normativa svizzera con rango di legge contiene diverse prescrizioni che specificano o circoscrivono i diritti delle persone coinvolte. Queste prescrizioni si applicano sia alla comunicazione nell'ambito delle reti sociali, sia alle informazioni diffuse tramite i canali usuali come giornali, radio, lettere o conversazioni telefoniche. Si pensi alle regole inerenti il diritto penale, civile (protezione della personalità) o sulla protezione dei dati. Le relative prescrizioni e la loro portata per i media sociali sono approfondite al punto 4 del presente rapporto.

2.4.2.2 Iscrivere nella legge sulle telecomunicazioni un regolamento specifico per i gestori di piattaforme?

Per determinati fornitori o trasportatori di informazioni il diritto svizzero prevede regole speciali che si applicano, ad esempio, alle emittenti di comuni programmi radiofonici e televisivi che soggiacciono alle disposizioni della legge sulla radiotelevisione (LRTV).

Le disposizioni particolari per la fornitura di servizi di telecomunicazione, ossia per il trasporto (la trasmissione) mediante tecnica delle telecomunicazioni di informazioni per terzi (anche di programmi radiotelevisivi) sono contenute nella legge sulle telecomunicazioni (LTC). Chiunque fornisce un servizio di telecomunicazione è tenuto a notificarlo all'Ufficio federale delle comunicazioni (art. 4 LTC), a soddisfare determinati requisiti organizzativi (art. 6 LTC), garantire l'obbligo del segreto delle telecomunicazioni (art. 43 LTC), partecipare a procedure di conciliazione (art. 12c LTC), garantire la trasparenza dei prezzi per gli utenti (art. 12a LTC), lottare contro la pubblicità di massa effettuata in modo sleale (art. 45a LTC) oltre che rispettare numerosi altri obblighi. La LTC è stata redatta ai tempi in cui la fornitura di servizi di telecomunicazione dipendeva dal possesso, o perlomeno dall'accesso autorizzato a un'apposita rete. I mutamenti tecnologici hanno spezzato questo stretto legame tra rete e servizi. La realtà odierna è completamente diversa, si pensi alle nuove possibilità di comunicazione date da Internet, dagli smartphone, ecc. I servizi possono essere erogati in svariati modi e senza il coinvolgimento attivo dell'operatore di rete, cosa che ha reso possibile modelli commerciali completamente nuovi come ad esempio il finanziamento tramite la pubblicità.

Secondo la legge vigente, offre servizi di telecomunicazione colui che trasmette mediante telecomunicazione informazioni per terzi (art. 3 lett. b LTC). In generale i gestori di piattaforme di media sociali non rientrano in questa categoria, ma rappresentano una delle parti, tra le quali vengono trasportate le informazioni. Vi sono però delle eccezioni in cui i gestori delle piattaforme sono perlomeno coresponsabili per il trasporto di informazioni tra terzi, cosicché, secondo la definizione in vigore, potrebbero rientrare nella categoria dei fornitori di servizi di telecomunicazione. Si pensi a una notizia che un membro di Facebook invia ad esempio tramite Facebook-Messenger a un altro membro di Facebook. A prescindere dalla difficoltà di imporre con gli strumenti attuali una legge nazionale sulle telecomunicazioni nei confronti di piattaforme attive su scala internazionale che non dispongono di una sede in Svizzera, molte delle regole di telecomunicazione vigenti non sono state concepite per disciplinare l'attività di queste piattaforme.

3 Potenziale e rischi delle reti sociali

3.1 In generale

La crescente presenza delle reti sociali digitali nella vita quotidiana di molte persone le rende oggetto di discussione e osservazione da parte di privati, Stati e organizzazioni multilaterali. Infatti, negli scorsi anni, sia il Consiglio d'Europa che l'Unione europea hanno rivolto un'attenzione particolare sul potenziale e sui rischi delle reti sociali.

3.2 Potenziale delle reti sociali

Le reti sociali consentono ai privati di produrre e diffondere contenuti in modo semplice, conveniente e rapido. Offrono possibilità d'intrattenimento, di scambio culturale e politico e di generare introiti. Hanno, inoltre, un potenziale capace di contribuire all'attivazione e alla mobilizzazione della popolazione, cosicché a sempre più persone singole sono date nuove opportunità di partecipare al discorso pubblico[18].

La *Corte europea dei diritti dell'uomo* ha sottolineato che, al giorno d'oggi, Internet è uno degli strumenti più importanti per pubblicare o procurarsi informazioni, soprattutto inerenti questioni politiche o altri temi d'interesse generale.[19]

Il *Consiglio d'Europa* ha elaborato una serie di raccomandazioni per i suoi 47 Stati membri tese ad aiutare il singolo nell'utilizzo di Internet e dei nuovi servizi di comunicazione (reti sociali comprese) per migliorare la percezione dei propri diritti fondamentali[20]. Occorre, ad esempio, promuovere le competenze mediali[21] della popolazione. Allo scopo di rafforzare la consapevolezza di tutti gli attori in quanto alla loro responsabilità nei confronti dei cittadini e sollecitarli a una migliore collaborazione, in ambito Internet e nuovi media, il Consiglio d'Europa collabora sempre più con l'economia e la società civile[22].

La Raccomandazione CM/Rec(2012)4 sulla protezione dei diritti dell'uomo nelle reti sociali [23] ribadisce la promozione della libertà d'informazione, d'opinione e di riunione attraverso le reti sociali e le loro innumerevoli possibilità tese a migliorare la partecipazione del singolo alla vita politica, sociale e culturale. In una raccomandazione sulla pluralità dei media il Consiglio d'Europa ha inoltre esplicitamente specificato che gli Stati membri sono tenuti a promuovere lo sviluppo delle reti sociali onde promuovere la pluralità dei media e creare spazi di dialogo[24].

Per garantire il funzionamento di un sistema di media indipendente e pluralistico nella società dell'informazione, il Consiglio d'Europa ha elaborato un nuovo concetto per i media che dovrebbe permette-

---

[18] Indicazioni quantitative si trovano ad esempio in Hilty/Oertel/Wölk/Pärli, *Lokalisiert und identifiziert*, Zurigo 2012, pag. 130 seg.

[19] Sentenza della Corte europea dei diritti dell'uomo sul caso «Ahmet Yıldırım c. Turchia» (n. 3111/2010) del 18.12.2012 relativa alla decisone di bloccare l'accesso alla piattaforma Google Sites contraria alla CEDU.

[20] http://www.coe.int/t/dghl/standardsetting/media/doc/cm_EN.asp .

[21] Per competenze mediali s'intende la facoltà di scegliere e fruire dei media, di capirne i contenuti e saperli valutare criticamente, capire l'economia dei media e riconoscere l'influenza dei media nonché saper comunicare in contesti variegati ed effettuare transazioni.

[22] Cfr. ad es. le linee guida sui diritti dell'uomo elaborate in collaborazione con i provider di servizi Internet e i produttori di giochi online: http://hub.coe.int/de/human-rights-guidelines-for-internet-service-providers-and-online-games-providers/ (in lingua inglese).

[23] Recommandation CM/Rec(2012)4 du Comité des Ministres du Conseil de l'Europe du 04.04.2012 sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux (Raccomandazione CM/Rec(2012)4 sulla protezione dei diritti dell'uomo nelle reti sociali).

[24] Raccomandazione CM/Rec(2007)2 sul pluralismo dei mezzi d'informazione e la diversità dei loro contenuti. La Corte europea dei diritti dell'uomo ha addotto questa raccomandazione ad esempio nella sua sentenza "Centro Europa 7 S.R.L. & Di Stefano c. Italia" (n. 38433/09) del 7.6.2012 (paragrafo 72, 134), che aveva in oggetto l'insufficiente pluralismo dei mezzi di comunicazione in Italia.

re, in forma adeguata e graduale, di applicare ai nuovi media, come ad es. ai media sociali, i principi base che stanno dietro alla tradizionale regolamentazione dei media[25].

Anche gli *Organi dell'UE* si interessano al variegato potenziale dei media sociali. Evidenziano infatti l'utilità delle piattaforme sociali per l'attuazione dei diritti umani, la partecipazione politica[26] e l'informazione indipendente dei media[27]. Sottolineano anche il carattere innovativo e creativo delle reti sociali nonché il loro significato per l'economia[28] e chiedono la promozione dell'utilizzo creativo di questi media[29].

3.3 Rischi delle reti sociali

L'egemonia di alcune poche piattaforme globali può implicare anche rischi, si pensi alla riduzione della pluralità dell'informazione e dell'opinione e al fatto che la dominanza sul mercato di una rete sociale venga sfruttata a fini politici o economici. Inoltre, i contenuti diffusi attraverso i media sociali possono mettere a repentaglio interessi individuali e pubblici (informazioni più dettagliate si trovano al Capitolo 4 di questo rapporto).

La Raccomandazione del Consiglio europeo sui servizi di social network localizza i rischi delle reti sociali soprattutto in relazione alla possibile amministrazione discriminante delle piattaforme sociali, ai pericoli per bambini e giovani e alla protezione precaria della sfera privata oltre che all'insufficienza della protezione dei dati.

Anche il *Comitato economico e sociale europeo (CESE)* definisce la mancanza di tutela della sfera privata e dei bambini e dei giovani uno dei maggiori problemi delle reti sociali[30]. Raccomanda l'introduzione, da parte delle istituzioni dell'UE, di disposizioni di auto o co-regolamentazione che, se attuate in modo insufficiente, dovranno essere convertite in prescrizioni vincolanti. Vista l'evoluzione dinamica delle reti sociali, per la regolamentazione delle piattaforme il CESE chiede la formulazione di prescrizioni generali, neutre sul piano tecnologico e auspica una promozione a tappeto delle competenze digitali della popolazione e l'ampliamento delle competenze delle hotline di Internet volte a sorvegliare l'uso improprio delle reti sociali.

---

[25] Recommandation CM/Rec(2011)7 du Comité des Ministres aux Etats membres sur une nouvelle conception des médias (Raccomandazione CM/Rec(2011)7 relativa a un nuovo concetto di media).

[26] Diritti umani e democrazia al centro dell'azione esterna dell'Unione europea — Verso un approccio più efficace, COM(2011) 886 definitivo, pag. 14, 20 seg. oppure i pareri del Comitato delle regioni «Servizio universale nelle comunicazioni elettroniche e internet e le reti del futuro», GU C del 28.5.2009, pag. 41 e Raccomandazione del Parlamento europeo del 26 marzo 2009 destinata al Consiglio sul rafforzamento della sicurezza e delle libertà fondamentali su Internet, (2008/2160(INI)), GU C 117 E del 6.5.2010, pag. 206.

[27] Risoluzione del Parlamento europeo del 7 settembre 2010 sul giornalismo e i nuovi media – creare una sfera pubblica in Europa, GU 308 E del 25.10.2011, pag 55.

[28] Parere del Comitato economico e sociale europeo «L'Internet degli oggetti» GU C 77 del 31.3.2009 pag. 60 o la comunicazione della Commissione intitolata «Relazione sulla competitività digitale in Europa: principali risultati della strategia i2010 nel periodo 2005-2009» COM(2009) 390 definitivo, pag. 10.

[29] Conclusioni del Consiglio, dell'11 maggio 2012, sulla promozione delle potenzialità di creatività e d'innovazione dei giovani, 2012/C 169/01, pag. 2. Vedi anche la comunicazione della Commissione intitolata «Relazione sulla competitività digitale in Europa: principali risultati della strategia i2010 nel periodo 2005-2009» (COM(2009)0390), pag. 12 o il Parere del Comitato delle regioni «Un'agenda digitale europea», pag. 38.

[30] Parere del Comitato economico e sociale europeo sul tema «Utilizzo responsabile delle reti sociali e prevenzione dei disturbi a queste associati», GU C 351 del 15.11.2012, pag. 31..

4 Attuale situazione legale nell'ambito delle reti sociali digitali

4.1 Premessa

Come illustrato precedentemente, le reti sociali possono dimostrarsi di grande utilità nella moderna società della comunicazione. Al contempo il loro utilizzo cela anche dei rischi, in parte di natura giuridica. Nelle pagine seguenti si affronteranno diversi problemi specifici alle reti sociali dal punto di vista degli utenti, degli altri soggetti indirettamente interessati e della collettività in generale. In seguito sarà presentato un ventaglio di soluzioni che sono state adottate all'estero o nel diritto internazionale e verrà analizzato l'attuale situazione legale in Svizzera.

4.2 Gestione discriminatoria delle reti sociali digitali

4.2.1 Condizioni di accesso problematiche e rifiuto di concedere l'accesso

4.2.1.1 Situazione iniziale

Per servirsi delle reti sociali si è spesso obbligati a fornire delle informazioni personali (quali ad es. nome e indirizzo di posta elettronica). La quantità e il contenuto delle informazioni richieste possono variare da una piattaforma all'altra. Il modello commerciale in uso (compravendita di dati personali) da una parte e dall'altra l'interesse che è suscitato dalla possibilità di controllare i contenuti della comunicazione all'interno della rete, accrescono l'interesse di molti gestori di piattaforme nei confronti di dati autentici relativi all'identità degli utenti. Se è vero che a volte gli interessati circuiscono le regole in materia di dati personali poste dai suddetti gestori, è probabile che nelle piattaforme dei media sociali la maggioranza degli utenti comunichi informazioni veritiere sulla propria identità. Divulgare queste informazioni può tra l'altro avere risvolti problematici se l'impiego a cui i dati personali sono potenzialmente destinati non è illustrato in modo trasparente.

I dati della registrazione possono riguardare anche futuri utenti, contenere informazioni che permettono di trarre conclusioni circa aspetti della loro identità e che possono indurre i gestori di piattaforme a rifiutarne l'accesso. Ciò risulterebbe problematico in particolare se l'esclusione dell'utente fosse da attribuire all'appartenenza a un determinato gruppo (basato, ad esempio, su distinzioni di razza, nazionalità, opinione politica, religione, inclinazione o genere sessuale, ecc.).

Immaginabile è anche l'esclusione di singoli individui indesiderati o di certe imprese dovuta a interessi di altra natura, in questo caso, economica. Tuttavia, essendo la gran parte delle reti sociali votata a modelli commerciali diretti ad ampliare il più possibile il numero dei propri membri, il rifiuto di concedere l'appartenenza alla rete rappresenta piuttosto un'eccezione.

4.2.1.2 Soluzioni adottate all'estero o nel diritto internazionale

La raccomandazione relativa alle reti sociali emanata dal Consiglio d'Europa mette in guardia dalle pratiche discriminatorie nel contesto delle reti sociali, che si possono concretizzare nell'esclusione di taluni utenti dalla piattaforma.

4.2.1.3 Situazione legale in Svizzera

Dal principio della libertà contrattuale deriva il diritto per i soggetti privati di decidere in sostanza liberamente a che condizione, con chi e su cosa si vuole stipulare un contratto[31]. Secondo la legislazione svizzera i gestori delle piattaforme sono fondamentalmente liberi di decidere con quale soggetto stipulare il contratto. Tale libertà contrattuale ha tuttavia dei limiti. In determinati casi un fornitore può essere obbligato a concludere contratti con persone interessate (il cosiddetto obbligo di contrarre).

L'obbligo di contrarre è espressamente disciplinato all'articolo 261bis CP, per cui è punito chiunque rifiuti a una persona o a un gruppo di persone, per la loro razza, etnia o religione, un servizio da lui offerto e destinato al pubblico (come nell'eventualità in cui il gestore di una piattaforma escludesse

[31] Schwenzer Ingeborg, *Schweizerisches Obligationenrecht Allgemeiner Teil*, sesta ed., Berna 2012, pag. 171 seg.

una comunità d'interesse in ragione delle sue origini etniche). In modo analogo l'articolo 6 della legge federale sull'eliminazione di svantaggi nei confronti dei disabili (legge sui disabili, LDis; RS *151.3*) vieta ai privati che forniscono prestazioni al pubblico di discriminare un disabile per la sua disabilità. La persona interessata può richiedere al giudice il versamento di un'indennità (art. 8 cpv. 3 LDis). Inoltre la legge permette alle organizzazioni di aiuto ai disabili d'importanza nazionale la facoltà di agire davanti alle istanze della giurisdizione civile per far accertare una discriminazione (art. 9 cpv. 3 lett. a LDis).

Gli obblighi legati alla conclusione del contratto trovano fondamento nella protezione della personalità sancita dal codice civile (art. 28, 28a cpv. 1 n. 2 CC) e nel divieto di cagionare ad altri un danno con atti contrari ai buoni costumi (art. 41 cpv. 2 CO)[32]. Il presupposto è da un lato che i beni o le prestazioni offerti e destinati al pubblico rientrino nelle necessità normali [33], dall'altro lato che alla parte richiedente manchino alternative accettabili a causa della posizione dominante del fornitore e che quest'ultimo non sia in grado di produrre alcuna motivazione oggettiva a giustificazione del rifiuto di stipulare il contratto[34].

Anche la normativa sui cartelli[35] circoscrive la libertà contrattuale, ma soltanto per le aziende che occupano una posizione dominante sul mercato. Sempre di più anche le imprese si avvalgono delle offerte dei social media, soprattutto per farsi pubblicità e per stabilire il contatto con i clienti. Se una rete sociale riuscisse a conquistare una posizione dominante sul mercato, per esempio nel mercato pubblicitario, il rifiuto di accordare l'accesso ad aziende interessate potrebbe eventualmente essere qualificato come rifiuto di relazioni commerciali (art. 7 cpv. 2 lett. a LCart) in contrasto con la legislazione sui cartelli.

Dall'analisi emerge che nel diritto svizzero i privati dispongono di ampie libertà per la conclusione di un contratto (in relazione alla controparte, al contenuto, ecc.), ma la legge pone un limite a questa libertà nel caso in cui una delle due parti arrivi a occupare una posizione di rilievo sul mercato oppure se la stipula del contratto sia negata in ragione di determinate caratteristiche della controparte. In queste eventualità è possibile esigere che il contratto venga stipulato in forza di legge.

4.2.2 Censura di contenuti da parte dei gestori delle reti sociali

4.2.2.1 Situazione iniziale

Nelle condizioni d'uso di numerosi gestori di reti sociali sono previste regole di comportamento che si applicano alla comunicazione sulla propria piattaforma nonché una lista di contenuti sottoposti a un generico divieto. Sono proibiti di solito tutti i contenuti a carattere pornografico, razzista, discriminatorio, offensivo o eccessivamente violento. Le reti sociali si rivolgono a un pubblico su scala globale e spesso adottano sistemi di vigilanza sui contenuti rispettosi degli ordinamenti giuridici di quasi tutti i Paesi in materia di contenuti illegali. Una possibile conseguenza è che certi contenuti vengano cancellati anche in Paesi in cui non creerebbero problemi di natura giuridica.

I metodi di vigilanza possono essere di diverse tipologie. Gli utenti hanno la possibilità di segnalare i contenuti sospetti, che saranno esaminati ed eventualmente cancellati dai gestori. Inoltre i gestori ricorrono spesso a software che filtrano e censurano automaticamente i contenuti. A seguito di violazioni un utente può vedersi cancellare definitivamente il proprio profilo. L'effetto di tutti questi rimedi può essere quello di eliminare contenuti di per sé innocui (come ad esempio la foto di una madre che allatta), un risvolto problematico in special modo nei casi in cui i contenuti pubblicati e condivisi non sono illegali né dannosi per la società, oppure se la loro consultazione è limitata a un ristretto gruppo di utenti.

---

[32] Schwenzer Ingeborg, *Schweizerisches Obligationenrecht Allgemeiner Teil*, sesta ed., Berna 2012, pag. 179 seg.

[33] Beni e servizi, oggigiorno praticamente a disposizione di tutti e d'uso quotidiano. Vedi DTF 129 III 35 consid. 6.3.

[34] DTF 129 III 35 consid. 6.3.

[35] Legge federale del 6 ottobre 1995 sui cartelli e altre limitazioni della concorrenza (legge sui cartelli, LCart), RS **251**.

4.2.2.2 Soluzioni adottate all'estero o nel diritto internazionale

La raccomandazione del Consiglio d'Europa relativa alle reti sociali richiede che gli utenti vengano informati in modo trasparente sui criteri redazionali applicati nel controllare i contenuti delle piattaforme, sul trattamento riservato a contenuti o comportamenti potenzialmente illegali o indesiderati e infine che i meccanismi di controllo in uso non limitino la libertà di opinione e di informazione in modo illecito. Nella sua dichiarazione sul rispetto della libertà di espressione, di riunione e di associazione in relazione alle piattaforme Internet gestite da privati, il Consiglio d'Europa mette in guardia oltretutto dal rischio che i fornitori di servizi Internet possano limitare i fondamentali diritti di comunicazione degli utenti sotto la spinta di pressioni politiche e porta all'attenzione degli Stati membri la gravità di eventuali limitazioni dei diritti fondamentali che potrebbero derivare da questa situazione. In aggiunta, il Consiglio d'Europa chiede che gli utenti siano avvisati in merito all'impiego di filtri sui contenuti in Internet, che vengano loro accordati il diritto di contestazione e di accertamento in relazione all'impiego di suddetti filtri ed eventualmente che sia loro permesso attuare controlli sul filtraggio stesso[36].

4.2.2.3 Situazione legale in Svizzera

Chi comunica contenuti a terzi può decidere liberamente quali contenuti trasmettere e quali no, nel rispetto di determinati vincoli giuridici. Se alcuni obblighi di trasmissione sono previsti dalla legge sulla radiotelevisione e dalla legge sulle telecomunicazioni, i gestori delle piattaforme di solito sono esonerati da queste prescrizioni. Inoltre possono emergere questioni che rientrano nel diritto della concorrenza: se un privato che occupa una posizione dominante sul mercato nega la trasmissione di determinati contenuti, ostacola illegalmente l'accesso o l'esercizio della concorrenza nei confronti del soggetto terzo, nel caso in cui l'impresa dominante non sia in condizione di fornire alcuna motivazione plausibile per il proprio rifiuto (ad es. i contenuti da comunicare sono illegali o contrari ai buoni costumi, mancanza di spazio ecc.) (art. 7 della legge sui cartelli, LCart). Nell'ipotesi che una rete sociale conquisti una posizione dominante sul mercato e sia per questo in condizione di decidere con grande arbitrarietà sulla comunicazione di contenuti, si presenta la questione se sia eventualmente possibile fissare delle prescrizioni in materia di trasmissione dei contenuti, analoghe agli obblighi esistenti per le emittenti radiotelevisive o agli obblighi di trasmissione di programmi per i fornitori di servizi di telecomunicazione. Un obbligo di trasmettere dei contenuti imposto per legge ai gestori delle piattaforme limita i loro diritti fondamentali (ad es. la libertà economica) e necessita delle consuete giustificazioni (art. 36 Cost.).

In circostanze particolari, ci si può opporre alla cancellazione di determinati contenuti in virtù del diritto d'autore (il diritto che compete all'autore) o appellandosi alla protezione della personalità del diritto civile (art. 28 CC).

Lo Stato può limitare il fondamentale diritto alla comunicazione anche indirettamente, frenando i privati nell'esercizio dei propri diritti. Ciò lascia supporre pertanto che uno stretto controllo sui contenuti da parte di un gestore possa essere indirettamente riconducibile anche a un intervento statale. Un quadro legale confuso, nel quale le disposizioni di legge restano vaghe, può a maggior ragione creare incertezza nei privati nel distinguere le affermazioni lecite da quelle illecite[37]. Il risultato è che, in mancanza di una chiara regolamentazione sulla responsabilità giuridica che fornitori di servizi Internet e gestori di piattaforme rivestono in relazione a contenuti diffusi da soggetti terzi, tali aziende procedono a cancellare in caso di dubbio anche quei contenuti che non infrangono la legge, nell'intento di evitare temute ripercussioni legali.

---

[36] Raccomandazione CM/Rec(2008)6 sulle misure volte a promuovere il rispetto della libertà di espressione e di informazione con riguardo ai filtri Internet.

[37] Müller Jörg Paul/Schefer Markus, *Grundrechte in der Schweiz*, quarta ed., Berna 2008, pag. 376.

4.3 Pregiudizio di altri interessi individuali cagionato dai gestori delle piattaforme

4.3.1 Problema fondamentale: carente controllo degli utenti sui propri dati

4.3.1.1 Situazione iniziale

In un'ottica giuridica di protezione dei dati il problema centrale si situa principalmente nell'insufficiente controllo che gli utenti possono operare sui propri dati[38]. Questa mancanza di controllo si manifesta in forme diverse:

Il grado di autonomia degli utenti quanto all'utilizzo dei propri dati non dipende soltanto dalla decisione di entrare a far parte di una rete sociale e di quali informazioni personali rivelino su questi siti.[39] Un ruolo centrale assume il tipo di programma messo a disposizione dai gestori di piattaforme. Il software infatti limita sistematicamente il controllo che gli utenti possono esercitare sui propri dati, applicando impostazioni carenti nella protezione della sfera privata. Un altro aspetto problematico risiede nel fatto che terzi, che hanno accesso al profilo di altri utenti, abbiano la possibilità di collocare in questi spazi testi e foto senza prima aver ottenuto il consenso del proprietario del profilo o ancora possano scaricare contenuti dai profili altrui a cui hanno accesso senza doverlo chiedere espressamente.

Un'altra strategia per sottrarre e complicare agli utenti il controllo sui propri dati è quello di richiedere il loro consenso a tutta una serie di trattamenti dei dati. La frequente introduzione di nuovi servizi e applicazioni da una parte e le costanti modifiche delle condizioni di utilizzo e delle dichiarazioni relative alla protezione dei dati dall'altra hanno la conseguenza che gli utenti debbano costantemente informarsi per conoscere le modalità di trattamento dei dati in uso. Di norma, le informazioni concernenti l'impiego dei dati del profilo e dei dati variabili sono difficili da trovare e spesso gli utenti non ricevono delucidazioni chiare sulla finalità del trattamento dei dati, l'eventuale trasmissione a terzi o semplicemente su come fare valere il proprio diritto d'informazione e alla rettifica dei dati.

Anche alle persone che non si servono delle reti sociali non è garantita una sufficiente protezione dei dati. Alcuni gestori di reti sociali (Facebook in particolare), infatti, consentono ai propri utenti di caricare all'interno del proprio profilo la lista dei contatti registrati sul telefono, sulla posta elettronica, ma anche sui servizi di messaggistica istantanea (funzione di ricerca degli amici). Questa funzione consente ai gestori delle piattaforme di verificare chi, fra i contatti comunicati, non si sia ancora affiliato alla rete. Di norma la piattaforma utilizza gli indirizzi forniti dopo aver richiesto il consenso dell'utente, allo scopo di inviare (indesiderati) messaggi pubblicitari e di invito a coloro i quali non si sono ancora registrati.

Il controllo è ulteriormente limitato dalla concessione di ampie facoltà ai suddetti gestori tramite le condizioni commerciali generali (CCG), che solitamente gli utenti sono tenuti a sottoscrivere per poter usufruire del servizio. Se il numero di reti sociali su Internet è esiguo o le piattaforme alternative risultano poco interessanti per via del limitato numero di utenti che vi partecipano, le condizioni d'uso restrittive dettate dai gestori risultano oltremodo problematiche. Numerose reti infatti prevedono un'ampia *concessione di diritti per l'utilizzo dei dati degli utenti*. La cancellazione dei contenuti da parte dell'utente di solito non cambia minimamente la situazione e può essere erroneamente interpretata da quest'ultimo come un'eliminazione definitiva dei propri contenuti (comprensiva della cancellazione dei dati sul server del gestore della rete).

---

[38] Cfr. in tal senso il rapporto Rapporto del Consiglio federale concernente la valutazione della legge federale sulla protezione dei dati del 9.12.2011 (FF **2012** 227, 242). Uno studio condotto dalla fondazione Warentest, esamina dieci tra le reti sociali più utilizzate sulla base di criteri come *organizzazione e trasparenza, trattamento dei dati degli utenti, sicurezza dei dati, diritti degli utenti, protezione dei giovani* e *lacune nelle condizioni generali,* ha riscontrato diverse carenze. Risultati negativi emergono soprattutto per le piattaforme statunitensi Facebook, LinkedIn e Myspace, ma anche per le reti tedesche Xing o Stayfriends. Vedi Stiftung Warentest *Datenschutz bei Onlinenetzwerken*, 2010; consultabile all'indirizzo: http://www.test.de/Soziale-Netzwerke-Datenschutz-oft-mangelhaft-1854798-0/ .

[39] Circa il 38 % degli utenti Internet in Svizzera dichiara di evitare la pubblicazione di dati personali sulle reti sociali. Vedi studio dell'Ufficio federale di statistica *Internet in den Schweizer Haushalten*. *Risultati dell'indagine Omnibus TIC 2010*, pagg. 47, 85.

Quali svantaggi possano derivare da un insufficiente controllo sui dati è esemplificato da un caso tratto dalla pratica di consulenza dell'IFPDT: l'organizzatore di un grande evento si è servito di una rete sociale su Internet come principale canale di comunicazione, ma il gestore della piattaforma ha cancellato la pagina della manifestazione poco prima dello svolgersi dell'evento. Non disponendo l'organizzatore di alcuna informazione per contattare i partecipanti al di fuori della rete sociale stessa, non ha più potuto dare la conferma definitiva dello svolgimento dell'evento. L'organizzatore non aveva alcun referente diretto presso il gestore della piattaforma, nonostante avesse pagato per la propria pagina. Ha dovuto perciò presentare la propria richiesta tramite un modulo di contatto generico che non ha più consentito di informare in tempo i partecipanti.

4.3.1.2 Soluzioni adottate all'estero o nel diritto internazionale

La raccomandazione del Consiglio d'Europa in merito alle reti sociali esige che i gestori delle piattaforme aumentino la trasparenza nel trattamento dei dati, ricevano il consenso informato del diretto interessato per ogni trattamento dei dati e spieghino agli utenti quando la loro comunicazione sia privata e quando pubblica. Inoltre gli utenti dovrebbero essere aiutati a comprendere le impostazioni che reggono le piattaforme sociali. Dovrebbero poter decidere consapevolmente in che misura i propri dati siano accessibili a terzi (*opt in*, *multi-layered access*). I gestori delle reti sociali dovrebbero astenersi dal raccogliere e dall'utilizzare i dati delle persone non affiliate (come ad esempio gli indirizzi di posta elettronica oppure i dati biometrici), adottare impostazioni di privatezza e programmi per l'interazione sociale volti alla protezione dei dati. Oltretutto gli utenti dovrebbero richiedere il consenso dei terzi, se intendono pubblicare contenuti che li riguardano.

La proposta dei comitati consultivi per la revisione della convenzione del Consiglio d'Europa del 28 gennaio 1981 per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale (RS *0.235.1*) sottolinea tra l'altro che le reti sociali e i blog necessitano di particolare attenzione[40]. Stando al progetto, un ampliamento dei diritti degli utenti dovrà accompagnarsi a una diversa concezione di servizi, prodotti e processi di lavoro, finalizzata a un trattamento dei dati conforme alla protezione dei dati. Inoltre si dovrà rafforzare il ruolo delle autorità preposte alla protezione dei dati, gli Stati membri del Consiglio d'Europa dovranno essere obbligati a fornire loro un adeguato sostegno personale, tecnico e finanziario, in modo da metterle in condizione di assolvere il proprio compito con efficienza e in piena autonomia[41].

Nel quadro della riforma della direttiva europea 95/46/CE relativa alla protezione dei dati personali[42] (che dovrebbe sfociare in un'ordinanza direttamente applicabile negli ordinamenti dei Paesi UE), sono previste diverse prescrizioni volte a migliorare il controllo degli utenti sui propri dati. Le norme proposte includono severi requisiti per ottenere il consenso in merito al trattamento dei dati per finalità precisamente definite, oltre a estesi obblighi d'accesso e d'informazione, riservando altresì particolare attenzione alla condizione dei bambini. Il progetto di ordinanza prevede la protezione dei dati tramite mezzi tecnici, impostazioni funzionali alla protezione dei dati (*privacy by design & privacy by default*), il principio di minimizzazione dei dati e limiti temporali per la loro registrazione[43].

---

[40] Modernisation of Convention 108, T-PD-BUR(2012)01Rev2_en, pag. 4.

[41] *Abridged Report of the Consultative Committee of Convention 108*, T-PD (2012) RAP 29 Abr_en, pag. 22 (art. 5), 24segg. (art. 7, 7^{bis}, 8, 8^{bis}), 29 (art. 12^{bis}).

[42] Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, pag. 31.

[43] Si rimanda all'art. 6 cpv. 1 lett. a, art. 7, 11, 14, 15, 23 Proposta UE di regolamento generale sulla protezione dei dati, COM(2012) 11 definitivo; vedi in tal senso per es. «Caspar Johannes, Soziale Netzwerke und Einwilligung der Nutzer», in: *digma* 2013/2, pag. 60 segg.

4.3.1.3 Protezione da una lesione della personalità causata da un trattamento di dati personali nella legislazione svizzera in materia di protezione dei dati

Ai sensi della legge federale sulla protezione dei dati (LPD; RS *235.1*), i contenuti che gli utenti mettono a disposizione nelle reti sociali si qualificano di norma come dati personali[44]. Spesso si tratta perfino di dati personali degni di particolare protezione [45] o di profili della personalità, a cui è riservata una protezione supplementare rispetto ai dati personali usuali. La legge sulla protezione dei dati tutela le persone fisiche e giuridiche anche da chi illecitamente lede la personalità con il trattamento di dati personali (art. 12 LPD). I gestori delle reti sociali digitali rientrano dunque, di principio, nel campo di applicazione della legge. Dato che spesso i gestori hanno la propria sede all'estero, le controversie in ambito civile relative alla competenza giurisdizionale vengono giudicate in base ad accordi internazionali[46] o alle disposizioni dell'articolo 129 segg. della legge federale sul diritto internazionale privato[47]. Inoltre occorre osservare che secondo la giurisprudenza del Tribunale federale[48], in caso di errori nel sistema l'incaricato federale della protezione dei dati e della trasparenza può chiarire una fattispecie soltanto se il trattamento dei dati ha in preponderanza stretti legami con la Svizzera.

Per quanto riguarda le reti sociali digitali si possono ipotizzare diversi tipi di violazioni dei principi che reggono il trattamento di dati personali (art. 12 cpv. 2 LPD). Eccone alcuni esempi:

- Se, all'acquisizione dei dati relativi a una persona, il gestore di una rete sociale non comunica che essi verranno venduti a terzi, che li potranno utilizzare a fini pubblicitari, oppure se non dichiara in modo trasparente la propria intenzione di esaminare e utilizzare i dati a scopo pubblicitario, commette normalmente una violazione dei principi dell'uso vincolato dei dati (art. 4 cpv. 3 LPD) e della riconoscibilità (art. 4 cpv. 4 LPD). Se l'esercente della rete sociale consegna i dati a terzi, nel trattamento dei dati essi sono a loro volta vincolati all'uso che era stato dichiarato al momento della loro raccolta a questi si applicano per analogia i vincoli che regolano la finalità di trattamento di suddette informazioni, quale era stata dichiarata all'atto della loro raccolta[49]; in aggiunta è illegale comunicare a terzi dati personali degni di particolare protezione o profili della personalità senza giustificazione (art. 12 cpv. 2 lett. c LPD).

- i principi della proporzionalità e dell'uso vincolato dei dati (art. 4 cpv. 2 e cpv. 3 LPD) possono essere infranti nel caso in cui gli esercenti delle reti sociali raccolgano, trattino e conservino più dati di quanti siano indispensabili per l'uso che essi hanno dichiarato. Inoltre il caposaldo della proporzionalità del trattamento dei dati acquista particolare rilievo nell'ottica di un utilizzo pubblicitario di dati personali degni di particolare protezione (trattandosi ad esempio dell'appartenenza a una razza, della sfera intima o di opinioni religiose o politiche; art. 3 lett. c LPD).

- Nell'eventualità in cui si verifichi un furto o una perdita di dati in una rete sociale digitale, dovuti al fatto che il gestore della piattaforma non ha messo in atto appropriati provvedimenti tecnici e organizzativi di sicurezza, si infrange il principio della sicurezza dei dati (art. 7 cpv. 1 LPD). Dal principio

---

[44] Conformemente all'art. 3 lett. a LPD sono dati personali tutte le informazioni relative a una persona identificata o identificabile. Conformemente a DTF 138 II 346 consid. 6.1., una persona infatti è identificabile se, pur non potendo essere individuata inequivocabilmente tramite i soli dati, sia comunque identificabile nella sua personalità in considerazione delle circostanze o del contesto di un'informazione o di altri elementi ancora (ad es. nel caso in cui i dati relativi all'immobile permettano di identificarne il proprietario).

[45] Secondo l'art. 3 lett. c LPD sono degni di particolare protezione i dati concernenti opinioni o attività religiose, filosofiche, politiche o sindacali, la salute, la sfera intima o l'appartenenza a una razza, le misure d'assistenza sociale, i procedimenti o le sanzioni amministrativi e penali.

[46] Per es. Convenzione del 30 ottobre 2007 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (CLug), RS **0.275.12**.

[47] RS **291**; CPC

[48] Cfr. DTF 138 II 346 consid. 3.

[49] *BSK-DSG*, Maurer-Lambrou Urs/Steiner Andrea, seconda ed., Basilea 2006, art. 4, pag. 83 n. marg. 16.

della sicurezza dei dati e dal principio della buona fede (art. 4 cpv. 2 LPD) deriva, in determinate circostanze, l'obbligo per il gestore della piattaforma di informare in materia di perdita e furto di dati[50].

- I principi che reggono il trattamento dei dati sono vincolanti anche per gli utenti. Ipotizziamo che, ad esempio, un utente carichi su una piattaforma sociale i contatti della lista telefonica e della posta elettronica o dei servizi di messaggistica istantanea: in osservanza ai principi che vincolano la finalità nel trattamento dei dati e ne prescrivono la riconoscibilità (art. 4 cpv. 3 e 4 LPD), insorge tanto per il gestore della piattaforma quanto per l'utente che pubblica i propri contatti l'obbligo di informare i soggetti coinvolti della raccolta di tali dati e del loro uso, se ciò non risulta evidente dalle circostanze.

- Se è vero che la LPD non prescrive un particolare regime di protezione per i fanciulli, il rispetto dei principi che reggono il trattamento dei dati, quali il caposaldo della riconoscibilità o quello della buona fede, pone tuttavia la necessità di dedicare all'elaborazione di dati personali relativi a un fanciullo maggiore attenzione di quella normalmente riservata al trattamento dei dati relativi a una persona adulta.

4.3.1.4 Giustificazione – in particolare il consenso al trattamento dei dati in primo piano

Un trattamento dei dati lesivo della personalità può essere giustificato da un preponderante interesse privato o pubblico, dalla legge o ancora se la persona lesa accorda il suo consenso (art. 13 cpv. 1 LPD). Stando al Tribunale federale non si può generalmente escludere una giustificazione per l'elaborazione di dati personali che vada contro i fondamentali principi che reggono il trattamento dei dati. Nella fattispecie comunque simili motivazioni possono essere accolte solo con ampie riserve[51].

Il trattamento dei dati da parte dei gestori di piattaforme sociali è in primo luogo giustificato dal consenso dell'interessato. Per poter usufruire dei servizi offerti nelle reti sociali digitali, è consuetudine che gli utenti dichiarino il proprio consenso in materia di diritto della protezione dei dati nelle condizioni commerciali generali CCG. In questo modo acconsentono sostanzialmente al trattamento dei dati illustrato dal gestore nelle disposizioni contrattuali. Tuttavia si possono sollevare questioni in merito alla validità e alla portata di tale consenso.

Ad esempio, possono sorgere problemi se è in dubbio la capacità di discernimento (art. 16 CC) di una persona in relazione al contenuto contrattuale, come nel caso dei *fanciulli* che rivelano dati relativi alla propria persona. I fanciulli incapaci di discernimento vengono rappresentati dai propri genitori, che esercitano l'autorità parentale. Si può quindi ipotizzare che, di principio, i genitori possano concedere al loro posto il consenso a determinate forme di trattamento dei dati (ad es. la pubblicazione su una rete sociale di foto che ritraggono un bambino in tenera età [52]).

I fanciulli capaci di discernimento possono agire autonomamente purché si tratti di diritti strettamente personali (art. 19c cpv. 2 CC), come i diritti della personalità legati al trattamento dei propri dati personali. In linea di massima, senza il consenso dei genitori possono rivelare informazioni su loro stessi contemplate dal diritto della personalità (si vedano le particolarità al punto 4.6.1.3). Affinché il consenso di un fanciullo capace di discernimento sia valido ai fini di un trattamento dei dati lesivo della personalità, il responsabile del trattamento dei dati dovrebbe formulare ed esporre le informazioni essenziali in modo tale da permettere al soggetto interessato di comprenderle a fondo. Inoltre, certi limiti possono essere posti anche al contenuto stesso del consenso, visti i frequenti cambiamenti delle finalità d'uso dei dati degli utenti e la difficoltà, talvolta, nel comprendere le dichiarazioni di protezione dei dati, senza dimenticare le conseguenze difficilmente calcolabili di determinate pratiche di trattamento dei dati.

---

[50] Rosenthal David/Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 82 n. 16.

[51] Vedi DTF 138 II 346 consid. 7.2 in riferimento a DTF 136 II 508 consid. 5.2.4.

[52] Per quanto riguarda la problematica dei diritti umani in tale situazione si rinvia alla fattispecie della sentenza della Corte europea dei diritti dell'uomo «Reklos & Davourlis c. Griechenland» (ricorso n. 1234/05) del 15.1.2009

Le condizioni generali, caratteristiche per la lunghezza e il registro linguistico, sono spesso sorvolate dagli utenti, che rinunciano a un'attenta lettura al momento di sottoscrivere il rapporto contrattuale. Nell'ipotesi in cui le condizioni commerciali generali fossero corredate da dichiarazioni di consenso conformi al diritto in materia di protezione dei dati e se queste ultime, alla stipula del contratto, fossero ignorate dagli utenti (accettazione globale), il linea di principio il consenso a clausole inusuali e senza legame con il contratto commerciale sarebbe nullo, a meno che non vi sia fatto specificamente riferimento[53]. In caso di dubbio, l'interpretazione di clausole oscure contenute nelle condizioni generali va a discapito di chi se ne avvale. Se non è possibile dare una chiara interpretazione di una condizione di utilizzo, si sceglie fra le soluzioni possibili quella più favorevole per gli utenti.

Il consenso a un trattamento dei dati lesivo della personalità è tale soltanto se è valido e non è stato revocato.[54]. Il consenso è considerato valido soltanto se è stato espresso prima del trattamento, liberamente e dopo debita informazione (ovvero in assenza di inganno, minaccia od obbligo)[55]; trattandosi di dati personali degni di particolare protezione o di profili della personalità, il consenso deve oltretutto essere esplicito (art. 4 cpv. 5 LPD). Per quanto riguarda le reti sociali digitali sono determinanti soprattutto la forma e il contenuto delle informazioni date all'utente, che devono essere chiare, oggettive, corrette, facilmente accessibili, ben riconoscibili e non fuorvianti[56].

Nel trattamento di dati personali usuali, il consenso può essere tacito, ossia si può dedurre dal comportamento di una persona che mette liberamente a disposizione i propri dati su una rete sociale.[57]. Il consenso deve tuttavia essere tanto più chiaro, quanto più sensibili sono i dati personali da elaborare[58]. Su Internet dovrebbe essere sufficiente dare il consenso a una dichiarazione in materia di protezione legale dei, una richiesta avanzata dalla maggior parte delle reti sociali, per soddisfare le esigenze formali di una chiara espressione del consenso[59].

Una volta espresso il proprio consenso alle condizioni di utilizzo delle reti sociali, gli utenti, a condizione di aver ricevuto adeguate informazioni, accettano di conseguenza l'effettiva modalità di funzionamento del servizio e quindi, ad esempio, anche il fatto che terzi pubblichino senza previa autorizzazione contenuti che li riguardano e sul proprio profilo. Nella misura in cui le attività condotte da terzi non violano il diritto vigente (ad es. nella forma di delitto contro l'onore, di violazioni al diritto alla propria immagine o del diritto di parola, di violazioni del segreto professionale ecc.), gli utenti di fatto non possono opporvisi. Una possibile reazione potrebbe essere quella di non partecipare a reti sociali che prevedono forme di comunicazione così aperte oppure eliminare contenuti spiacevoli dal proprio profilo. Dal momento che un determinato contenuto ha suscitato forte interesse nella comunità della rete sociale, l'utilità di una cancellazione resta tuttavia limitata, se il contenuto è già stato ripetutamente copiato o è oggetto di molti rinvii ipertestuali.

4.3.1.5 Dati personali pubblicamente accessibili

Sono pubblicamente accessibili i dati personali di cui un numero indeterminato di persone può venire a conoscenza senza particolari ostacoli. Di norma, non vi è lesione della personalità se gli utenti svelano dati sulla propria persona nelle reti sociali, a patto che abbiano reso i propri dati accessibili a chiunque in piena coscienza e volontà e non si siano opposti espressamente al trattamento (art. 12

---

[53] *BSK-DSG*, Rampini Corrado, seconda ed., Basilea 2006, art. 13, pag. 194 n. marg. 13 e Rosenthal David/Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 112 n. 90.

[54] Rosenthal David/Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 386 n. 3.

[55] Un parere estremamente critico sulle dichiarazioni relative alla protezione dei dati di Facebook è espresso in: Baeriswyl Bruno, «Kleingedrucktes unter der Lupe - Die Allgemeinen Geschäftsbedingungen (AGB) von Sozialen Netzwerken versprechen keinen Datenschutz», in: *digma* 2010 pag. 56, 59 e Caspar Johannes, «Soziale Netzwerke und Einwilligung der Nutzer», in: *digma* 2013/2, pag. 63 seg.

[56] Rosenthal David/Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 106 n. 75.

[57] Rosenthal David/Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 108 n. 79.

[58] FF **2003** 1909 seg.

[59] Rosenthal David/Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 108 n. 78.

cpv. 3 LPD). Questo principio vale anche per la comunicazione di dati personali all'estero in Paesi che offrono garanzie insufficienti per la protezione dei dati (art. 6 cpv. 2 lett. f LPD).

Per quanto concerne l'accessibilità delle informazioni, in sostanza gli utenti possono scegliere liberamente tra le diverse impostazioni di utilizzo proposte. Nella maggior parte delle reti sociali esiste la possibilità di scegliere fra diverse forme di comunicazione a cui sono associati diversi livelli di riservatezza, su una scala che spazia dalla comunicazione privata a quella di massa. Posto che gli utenti siano stati adeguatamente informati sulle diverse forme di comunicazione disponibili e sul relativo grado di privatezza che le contraddistingue, a seconda della forma di comunicazione che hanno adottato, si può giudicare se la comunicazione era intesa a carattere privato oppure se si voleva rendere le informazioni di dominio pubblico.

Anche il trattamento di dati personali resi accessibili a chiunque può costituire una lesione della personalità, quando il trattamento dei dati esula dallo scopo per cui, considerate le circostanze e sulla base di un esame oggettivo, tali dati erano stati resi pubblici[60]. Questo aspetto è importante per i dati che sono accessibili a chiunque su Internet in particolare perché facilmente reperibili[61]. Anche il fatto che una persona pubblichi delle foto su una rete sociale, rendendole di fatto visibili per chiunque, non ne consente tuttavia l'utilizzo senza autorizzazione per la campagna pubblicitaria di un'azienda. L'utilizzo di questa categoria di foto presenta dei problemi anche nell'ambito del giornalismo nei media tradizionali.[62]

Dati questi presupposti, a ogni singolo caso si ripropone la questione se scaricare e registrare i contenuti dai profili di estranei senza chiederne prima l'autorizzazione possa ancora rientrare nelle finalità di pubblicazione. Vale ad ogni modo il principio che gli altri membri della rete sociale, così come il gestore della piattaforma, devono attenersi ai principi che reggono il trattamento dei dati.

4.3.1.6 Il problema specifico del trasferimento di diritti di utilizzo di vasta portata ai gestori delle piattaforme

Se il contratto concluso fra utente e gestore della piattaforma riguarda espressamente la conservazione illimitata e l'utilizzo di tutti i contenuti pubblicati dagli utenti nelle reti sociali, ci si interroga in merito alla validità di un simile contratto. Non si può escludere che un simile contratto nella fattispecie possa essere qualificato come negozio giuridico contrario ai diritti inerenti alla personalità (art. 19 cpv. 2 e art. 20 cpv. 1 CO; art. 27 cpv. 2 CC), tanto più che i dati pubblicati nelle reti sociali e che divengono poi oggetto di rinvii ipertestuali spesso appartengono alla categoria dei dati degni di particolare protezione, oppure caratterizzano il profilo della personalità, e che sollevi delle questioni sul rapporto tra prestazione e controprestazione (offerta di un'infrastruttura di comunicazione da parte del gestore della piattaforma in contropartita a un trasferimento di diritti di vasta portata concernenti l'utilizzo dei dati personali degli utenti)[63]. Sotto questo profilo assume un'influenza sostanziale il fatto che gli utenti abbiano un considerevole margine di scelta su quali dati pubblicare nelle reti sociali.

4.3.1.7 Ulteriori strumenti di protezione previsti dalla legislazione svizzera

Accanto alla legge sulla protezione dei dati, l'ordinamento svizzero dispone di ulteriori strumenti per la protezione dei dati da metodi non trasparenti di raccolta, trattamento e pubblicazione praticati dai gestori delle reti sociali. Basta prendere in considerazione, ad esempio, gli strumenti di **contestazione**

---

[60] Rosenthal David/Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 381 n. 76.

[61] *BSK-DSG*, Rampini Corrado, seconda ed., Basilea 2006, art. 12, pag. 187 seg. n. marg. 18.

[62] In veste di organo istituzionalizzato di auto vigilanza nel giornalismo, il Consiglio svizzero della stampa ha esortato a più riprese i giornalisti ad astenersi dall'utilizzo di informazioni pubblicate in Internet da privati. Chi rende pubbliche immagini su blog o su un'altra piattaforma accessibile a tutti, non approva semplicemente la loro ulteriore diffusione tramite un altro mezzo di comunicazione. I giornalisti dovrebbero anche considerare accuratamente la tutela della vita privata contro l'interesse della collettività in materia d'informazione; cfr. per es. il parere del Consiglio svizzero della stampa n. 43/2010 del 1.9.2010: Internet e la sfera privata; http://www.presserat.ch/28380.htm.

[63] Schwenzer Ingeborg, *Schweizerisches Obligationenrecht Allgemeiner Teil*, sesta ed., Berna 2012, pag. 256 seg.

del contratto previsti dal diritto privato in presenza di un errore essenziale (CO; art. 23 segg.) o di dolo (art. 28 CO)[64].

Inoltre praticare condizioni commerciali abusive può costituire una pratica d'affari sleale (art. 8 della legge federale del 19 dicembre 1986 contro la concorrenza sleale [**LCSl**], RS *241*). Ai sensi dell'ultima modifica della LCSl del 1° luglio 2012 è sleale qualsiasi utilizzo delle condizioni commerciali generali che viola il principio della buona fede se comporta a detrimento dei consumatori un notevole e ingiustificato squilibrio tra i diritti e gli obblighi contrattuali[65]. La nuova versione elimina il requisito dell'induzione in errore precedentemente sancito all'articolo 8 LCSl (prova della minaccia di inganno), cosicché ora è possibile esercitare un controllo esplicito del contenuto delle CCG rivolte ai consumatori[66]. Per quanto riguarda le CCG dei fornitori di servizi nei media sociali, si pone ad esempio la questione se le clausole che permettono la modifica unilaterale delle condizioni di utilizzo da parte dei gestori delle piattaforme senza comunicazione di scadenza o qualsivoglia informazione sarebbero ancora conformi al nuovo articolo 8 LCSl.

La violazione reiterata e ingiustificata dei principi che reggono il trattamento dei dati nella legge sulla protezione dei dati potrebbe essere sleale anche ai sensi dell'articolo 2 LCSl, nella circostanza in cui un trattamento dei dati non consentito dalla LCSl permetta, a chi lo esegue, di ottenere un vantaggio nei confronti dei propri concorrenti[67]. Si pensi a titolo di esempio ai dati personali che, in violazione delle norme di protezione, vengono raccolti nelle reti sociali, trattati e venduti a scopi pubblicitari.

4.3.1.8 Apprezzamento giuridico

Nel complesso si può affermare che il diritto svizzero vigente, grazie a prescrizioni di protezione formulate in modo aperto, tutela in buona misura dalle pratiche di trattamento dei dati che usualmente creano problemi nelle reti sociali. D'altro canto si rilevano diverse difficoltà, rilevanti anche per i media sociali, che ostacolano un'efficace protezione dei dati. A questo titolo si fa riferimento, ad esempio, alla spesso insufficiente riconoscibilità di trattamenti dei dati problematici, all'enorme aumento del trattamento dei dati su scala internazionale (una pratica che complica notevolmente sia l'istruttoria sia i procedimenti esecutivi; si veda a tal proposito il successivo capitolo 5) e alla probabilità, proporzionalmente assai ridotta, di incorrere in sanzioni. Si aggiunga che gli utenti, di fatto, non esercitano i propri diritti azionabili e che le risorse l'IFPDT giungono ai loro limiti tanto sono numerosi i casi rilevanti[68].

Dei miglioramenti si potrebbero ottenere anche, ad esempio, adottando preimpostazioni che consentano una maggiore protezione dei dati (*privacy by design* e *privacy by default*) e una formulazione più comprensibile delle dichiarazioni di protezione dei dati. Nel rapporto di valutazione della LPD il Consiglio federale ha prospettato in primo luogo un approfondimento del concetto di *privacy by design*, ossia la progettazione di nuove tecnologie nell'ottica della protezione dei dati, in secondo luogo la promozione di tecnologie funzionali alla protezione dei dati e infine l'adozione di misure per migliorare il controllo e il dominio sui dati.[69]

---

[64] A proposito di questi rimedi giuridici si rimanda a: Schweizer Alex, «Data Mining – ein rechtliches Minenfeld. Rechtliche Aspekte von Methoden des Customer Relationship Management (CRM) wie Data Mining», in: *digma* 2001 pag. 108, 111-114.

[65] RU **2011** 4910

[66] Attraverso la soppressione dell'elemento dell'inganno si intendono ora creare i presupposti per un controllo esplicito del contenuto (FF **2009** 5363).

[67] Weber Rolf/Volz Stephanie, *Online Marketing und Wettbewerbsrecht*, Zurigo 2011, pag. 65 seg.

[68] Rapporto del Consiglio federale concernente la valutazione della legge federale sulla protezione dei dati del 9 dicembre 2011 (FF **2012** 232-235, 238-239).

[69] Rapporto del Consiglio federale concernente la valutazione della legge federale sulla protezione dei dati del 9 dicembre 2011 (FF **2012** 239)

4.3.2 Creazione e gestione di profili degli utenti esaustivi (Data Mining)

4.3.2.1 Situazione iniziale

Gli utenti rivelano un grande numero di informazioni su se stessi, vuoi tramite le procedure di registrazione, vuoi interagendo nelle reti sociali, vuoi con la navigazione in Internet, le cui tracce restano nei metadati (durata del collegamento, origine geografica approssimativa dell'indirizzo IP, permanenza e movimenti su un sito Web, ecc.). L'attivazione del pulsante facebook «mi piace» sulle pagine Web di terzi consente di raccogliere dati sui visitatori di questi siti.

Nel caso di numerosi gestori delle piattaforme non è chiaro come vengano utilizzati i dati raccolti. Riunire tutte le informazioni, ossia le tracce rimanenti dell'utilizzo delle reti sociali può servire a comporre profili indicativi, anche se non privi di errore. Se il gestore della piattaforma vende pacchetti di dati a terzi, allora i profili possono essere utilizzati come base per offrire servizi e prodotti, il che pone dei problemi non soltanto a causa della strumentalizzazione economica dei dati ma anche a causa del potenziale di discriminazione.

4.3.2.2 Soluzioni adottate all'estero o nel diritto internazionale

La raccomandazione del Comitato dei Ministri del Consiglio d'Europa sulla protezione delle persone nell'ambito del trattamento automatico di dati personali per la creazione di profili[70] tratta l'osservazione, la raccolta e la concordanza di dati a carattere personale in Internet e chiede un'estesa protezione giuridica dei soggetti coinvolti. Le reti sociali rappresentano una ricca miniera da cui attingere per questo tipo di trattamento dei dati. Il Consiglio d'Europa individua la problematicità nella mancanza di trasparenza alla creazione del profilo, nella possibile discriminazione dei soggetti interessati e anche nell'insufficiente protezione dei bambini da questo genere di raccolta dei dati. Lancia inoltre un appello affinché sia possibile accedere a prodotti e servizi (e alle relative informazioni) senza dover fornire dati a carattere personale non necessari alla fornitura dei suddetti servizi o prodotti. Chi fornisce servizi nell'ambito della società dell'informazione dovrebbe inoltre garantire la libera consultazione delle informazioni sui propri servizi senza la creazione di un profilo.

L'articolo 20 della proposta UE di regolamento generale sulla protezione dei dati[71] è volto alla protezione delle persone fisiche (prevedendo alcune eccezioni) dal trattamento automatizzato dei dati al fine di analizzare o prevedere taluni aspetti della personalità o della situazione di vita. Presupposto a tale protezione è che tale trattamento nuocia significativamente alla persona coinvolta e produca effetti giuridici nei sui confronti. Qualora i dati personali siano trattati per finalità di marketing diretto, ai sensi dell'articolo 19 capoverso 2 della proposta, l'interessato ha il diritto di opporsi gratuitamente a tale trattamento.

L'autorità degli Stati Uniti d'America responsabile per la protezione dei consumatori e il diritto alla concorrenza (Federal Trade Commission FTC) ha esortato l'industria Internet ad allestire un'opzione di non tracciabilità (*Do-Not-Track*), con cui si lascerà ai consumatori la scelta in merito a quali informazioni sulle proprie attività online debbano essere comunicate, a chi e a che scopo (in primo piano vi sono le misure di marketing diretto) [72].

---

[70] Raccomandazione CM/Rec(2010)13.

[71] Proposta di Direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), COM(2012) 11 definitivo.

[72] «Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers», *FTC Report March 2012*; consultabile all'indirizzo: http://www.ftc.gov/opa/2012/03/privacyframework.shtm . Il rapporto sulla protezione della sfera privata dei consumatori in Internet contiene proposte di direttive all'attenzione dell'industria di Internet, in cui si esige anche che le imprese sviluppino i propri servizi Internet in vista di un più elevato standard di protezione della sfera privata (privacy by design) e che i consumatori ricevano ampi chiarimenti sullo scopo, la portata e il tipo di utilizzo dei dati.

Il Trans Atlantic Consumer Dialogue (TACD)[73] ha redatto una risoluzione sulle reti sociali[74] che richiede l'emanazione di norme di legge le quali tra l'altro prevedono che le reti sociali svincolino l'accesso ai propri servizi dal consenso degli utenti all'impiego dei propri dati a fini di marketing. Inoltre dovrà essere obbligatorio richiedere l'esplicito consenso degli utenti per la raccolta di dati a fini pubblicitari, e in linea di principio i messaggi pubblicitari non dovranno essere visualizzati dai minori di 16 anni. I siti Web che sono visitati prevalentemente da questo giovane pubblico dovranno essere privi di contenuti pubblicitari.

4.3.2.3 Situazione legale in Svizzera

La raccolta e il raggruppamento di dati che gli utenti producono con la loro attività porta in molti casi alla creazione di profili della personalità ai sensi dell'articolo 3 lettera d LPD. La legge sulla protezione dei dati fissa particolari requisiti per il trattamento di profili della personalità (art. 4 cpv. 5, art. 11a cpv. 3 lett. a, art. 12 cpv. 2 lett. c, art. 14 LPD).

Se, ricongiungendo i dati, gli esercenti delle piattaforme creano profili della personalità, essi possono commettere una violazione del principio della buona fede a causa dell'insufficiente riconoscibilità di questa operazione (art. 4 cpv. 2 LPD). In questa circostanza, inoltre, trova applicazione l'obbligo d'informazione che, nell'ambito della raccolta di profili della personalità, il detentore di una collezione di dati ha nei confronti della persona interessata (art. 14 LPD). Anche trasmettere a Facebook i dati degli utenti, creando il collegamento ipertestuale con il pulsante «mi piace» sulle pagine Web di terzi, può costituire una violazione del principio della riconoscibilità (art. 4 cpv. 4 LPD), in quanto il visitatore del sito non è sufficientemente informato a proposito della successiva trasmissione dei dati. Oltretutto, indicare finalità di trattamento molto generiche quando si procede alla raccolta dei dati, quali ad esempio la creazione e il trattamento di profili degli utenti *a scopo pubblicitario*, può non soddisfare sufficientemente il principio dell'uso vincolato (art. 4 cpv. 3 LPD). Al momento della raccolta dei dati, gli utenti spesso non sono sufficientemente a conoscenza dello scopo a cui saranno successivamente destinati i dati collegati ai profili utente.

Collezionare una grande quantità di dati personali e ricongiungerli per creare profili della personalità può infrangere il principio della proporzionalità nel trattamento dei dati (art. 4 cpv. 2 LPD). Analogamente, la creazione di profili della personalità può confliggere con il principio dell'esattezza dei dati (art. 5 LPD): la raccolta, la composizione e la valutazione automatizzate di dati provoca la perdita del contesto originario in cui sono stati creati e, in determinate circostanze, può produrre false dichiarazioni[75].

Un aspetto di capitale importanza nell'ambito dei profili della personalità è che il consenso dell'interessato deve essere esplicito (art. 4 cpv. 5 LPD). Questo requisito aumenta le esigenze in materia di informazione sulla creazione, sull'impiego e sulla trasmissione di profili della personalità, soprattutto se vi è fatto riferimento nelle CCG. Lecito sarebbe infatti dubitare della validità di un esplicito consenso che è stato accordato in presenza di finalità del trattamento o di comunicazione a terzi inusuali e non adeguatamente segnalate. Un consenso esplicito da parte dell'interessato è indispensabile quando si debba giustificare un trattamento di profili della personalità in aperto contrasto con i principi che reggono il trattamento dei dati o la comunicazione di profili della personalità a terzi (art. 13 cpv. 1 in combinato disposto con l'art. 4 cpv. 5 LPD). In relazione alle reti sociali questo aspetto acquisisce una rilevanza speciale, in quanto i loro modelli commerciali sono normalmente basati sulla vendita di profili degli utenti, un'operazione qualificata come comunicazione di dati a terzi.

---

[73] Il TACD è un forum che riunisce le associazioni dei consumatori statunitensi ed europee, rivolto all'emanazione di raccomandazioni a protezione dei consumatori destinate al governo degli USA e all'Unione europea; cfr.: http://www.tacd.org/ .

[74] *Resolution on Social Networking of May 2010*, Doc No. Infosoc 43-09; consultabile all'indirizzo: http://tacd.org/index.php?option=com_docman&task=cat_view&gid=83&Itemid=40 .

[75] Schweizer Alex, «Data Mining – ein rechtliches Minenfeld. Rechtliche Aspekte von Methoden des Customer Relationship Management (CRM) wie Data Mining», in: *digma* 2001 pag. 108, 109.

La LPD non predispone una protezione speciale per i fanciulli in relazione alla creazione e al trattamento di profili della personalità. A questo proposito bisogna tuttavia tener conto degli aspetti peculiari che caratterizzano il consenso al trattamento di dati personali di un fanciullo (vedi sopra punto 4.3.1.3.). In linea di principio non esistono prescrizioni che vietino di fare pubblicità per i minori di 16 anni o su pagine Web dedicate a questo pubblico.

L' **obbligo del segreto** all'articolo 43 LTC e all'articolo 321ter CP protegge la segretezza delle telecomunicazioni, ma in linea di massima non tutela dalla creazione di profili della personalità. Soltanto in casi eccezionali, in cui i gestori delle piattaforme trasportino informazioni tra diversi utenti, l'obbligo del segreto nelle telecomunicazioni potrebbe proteggere questi utenti dalla trasmissione a terzi dei dati relativi al proprio traffico di comunicazione e dalla loro utilizzazione per la creazione di profili degli utenti.

4.3.3 Insufficiente diritto all'oblio

4.3.3.1 Situazione iniziale

La mancanza di controllo degli utenti sui propri dati nelle reti sociali si manifesta tra l'altro nella difficoltà di cancellare definitivamente il profilo dell'utente. Nella maggior parte dei casi, cancellare un conto determina soltanto la disattivazione del profilo, mentre i dati registrati sul server del gestore della piattaforma continuano a essere conservati. La cancellazione definitiva di tutti i contenuti è certo frequente, ma non sempre possibile. Il procedimento oltretutto si presenta così complicato e poco comprensibile da scoraggiare chi lo volesse effettuare. Per di più gli utenti attivi hanno la possibilità di lasciare un gran numero di informazioni e di contenuti su altre pagine e profili della rete. Eliminarli completamente è di fatto praticamente impossibile.

L'utilità di un'eventuale cancellazione del profilo originale è sminuita peraltro dalla possibilità, predisposta da alcune piattaforme, di scaricare e registrare i dati degli altri profili degli utenti. Ciò rende possibile la creazione di un numero indefinito di collezioni private di dati. Anche se gli utenti cancellano il proprio profilo originale, i loro dati possono continuare a essere memorizzati in un'altra sede. Inoltre soggetti terzi dispongono di altre possibilità per archiviare i dati (ad es. copiando l'immagine dello schermo) ed per eventualmente ripubblicarli successivamente.

4.3.3.2 Soluzioni adottate all'estero o nel diritto internazionale

Tanto la raccomandazione del Consiglio d'Europa in merito alle reti sociali quanto la proposta UE di regolamento generale sulla protezione dei dati[76] prevedono, date alcune condizioni, il diritto all'oblio, alla cancellazione di dati a carattere personale nonché di rinunciare a un'ulteriore diffusione di tali dati[77]. In particolare è contemplato il diritto all'oblio e alla cancellazione dei dati78 per i minori [1].

Anche il progetto di modifica della legge tedesca sui mezzi di telecomunicazione prevede il diritto alla cancellazione di conti utente nelle reti sociali e di tutto l'insieme dei contenuti generati dagli utenti[79].

4.3.3.3 Situazione legale in Svizzera

Il diritto all'oblio nelle reti sociali rappresenta fondamentalmente la richiesta di cancellazione effettiva dei contenuti pubblicati dagli utenti delle reti sociali. Il diritto alla cancellazione poggia le sue basi tanto sulla legge sulla protezione dei dati quanto sulla protezione della personalità del diritto civile.

---

[76] Art. 17 Proposta UE di regolamento generale sulla protezione dei dati, COM(2012) 11 definitivo.

[77] Cfr. al proposito Treyer Tobias, «Das „Recht auf Vergessen“ im digitalen Zeitalter», in: *medialex 2013*, pag. 61 seg.

[78] Art. 17 cpv. 1 Proposta UE di regolamento generale sulla protezione dei dati, COM(2012) 11 definitivo. Si veda anche Déclaration du Conseil de l’Europe sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur l'Internet.

[79] Progetto per la modifica della Telemediengesetz 17/6765.

Il **diritto alla protezione dei dati** vieta il trattamento di dati a carattere personale contro l'esplicita volontà di una persona (art. 12 cpv. 2 lett. b LPD). Siccome la registrazione e l'archiviazione di dati personali possono essere oggetto di un espresso divieto di trattamento, in forza del diritto di opposizione è di principio legittima anche la richiesta di cancellare del tutto o parzialmente i dati personali[80]. Anche il consenso di cui all'articolo 13 capoverso 1 LPD, tramite cui i trattamenti dei dati lesivi della personalità sono giustificati, può essere revocato. La revoca ha tuttavia effetto solo per trattamenti dei dati futuri, non per quelli già compiuti[81]. Se, quindi, si acconsente alla conservazione senza limiti temporali dei dati, si può sempre revocare questo consenso per i dati che saranno registrati in futuro.

Nell'eventualità in cui, senza giustificato motivo, soggetti terzi contravvengano ai principi che reggono il trattamento dei dati della legge sulla protezione dei dati, un diritto alla cancellazione dei dati interessati può essere desunto dall'articolo 15 capoverso 1 LPD. A titolo esemplificativo si considerino i casi in cui altri utenti pubblicano sulle reti sociali i dati personali degli interessati, senza che ciò sia riconoscibile da questi ultimi (art. 4 cpv. 2 e 4 LPD). È inoltre possibile che dati personali degni di particolare protezione o profili della personalità di un soggetto siano comunicati ad altri membri della rete o a imprese terze senza giustificazione (art. 12 cpv. 2 lett. c LPD), che i dati di una persona siano trattati per uno scopo differente da quello riconoscibile all'atto della loro raccolta (quando, ad esempio, delle affermazioni rilasciate nell'ambito di una rete sociale digitale in un forum o in relazione a un determinato tema vengono ripresentate fuori contesto con finalità del tutto diverse)[82] oppure che dati personali vengano trattati contro l'esplicita volontà dell'interessato (art. 12 cpv. 2 lett. b LPD).

Anche nella **protezione della personalità del diritto civile** (art. 28 CC) si possono individuare elementi a sostegno di un diritto di cancellazione che, per altro verso, dipendono da valutazioni sugli interessi in gioco o dall'esistenza o meno di motivi giustificativi che annullino l'illegittimità di una lesione della personalità. L'articolo 28 del Codice civile comprende diversi contenuti parziali. Il diritto all'oblio può essere fatto valere appellandosi alla protezione dell'integrità morale, della sfera privata, dell'onore, del diritto alla propria immagine, al proprio nome o del diritto di parola. L'articolo 28 del Codice civile sancisce il divieto per terzi di acquisire o pubblicare contenuti che appartengono alla sfera personale segreta o privata oppure foto di una persona senza il suo consenso (o senza altro valido motivo giustificato). L'articolo 28a capoverso 1 numero 2 del Codice civile sancisce il diritto degli interessati di far cessare una lesione attuale e perciò, in linea di principio, il potere di ottenere anche una cancellazione di contenuti lesivi della personalità su Internet. Se gli utenti pubblicano sulle reti sociali contenuti che li riguardano e che vengono successivamente trattati da terzi, è necessario tenere presente che il consenso accordato per una determinata finalità di impiego non si estende anche ad altre finalità[83]. Nell'ottica del diritto civile si riscontrano dei problemi, ad esempio, se le affermazioni rilasciate da una persona vengono usate come false citazioni[84], quando si fa uso in un altro contesto o per un altro scopo delle foto pubblicate da qualcuno senza averne previamente ottenuto il consenso[85] oppure quando il nome di una persona è utilizzato in modo da lederne la personalità[86]. Si può quindi ritenere che il consenso accordato una volta può essere revocato, mentre, anche qui, l'esistenza di un diritto di cancellazione dipende da concrete considerazioni degli interessi[87].

---

[80] Rosenthal David / Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 362 n. 32.

[81] Rosenthal David/Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 118segg. n. 104segg.

[82] Questo atto potrebbe analizzato nell'ottica dei principi dell'uso vincolato e dell'esattezza dei dati (art. 4 cpv. 3 e 5 LPD).

[83] *BSK-ZGB I*, Meili Andreas, 4 ed., Basilea 2010, art. 28, pag. 269 n. marg. 48.

[84] Schweizer Michael, «Das Recht am Wort nach Art. 28 ZGB», in: *medialex 2011* pag. 197, 199.

[85] *BSK-ZGB I*, Meili Andreas, 4 ed., Basilea 2010, art. 28, pag. 260 n. marg. 20 si fa altresì riferimento al fatto che, nella pratica, pongono sempre e comunque difficoltà i ritocchi digitali e tradizionali, i fotomontaggi e vere e proprie manipolazioni dell'immagine, così come l'impiego di foto d'archivio in un contesto completamente estraneo a quello del momento in cui è stata scattata la fotografia.

[86] *BSK-ZGB I*, Meili Andreas, 4 ed., Basilea 2010, art. 28, pag. 320 n. marg. 1.

[87] *BSK-ZGB I*, Meili Andreas, 4 ed., Basilea 2010, art. 28, pag. 259 n. marg. 48.

L'esistenza di un eventuale diritto alla cancellazione è legata anche alla modalità, scelta dal soggetto interessato, di pubblicare i contenuti in questione (comunicazione privata o pubblica?), alla natura dei contenuti (appartengono alla sfera segreta, privata o pubblica?) e alla tipologia di persona che è direttamente coinvolta. Se i contenuti sono stati pubblicati direttamente dagli interessati (ai sensi dell'art. 12 cpv. 3 LPD), nella valutazione di un'eventuale richiesta di cancellazione dovrebbe essere tenuto debito conto di tale circostanza a sostegno del gestore della piattaforma (art. 13 cpv. 1 LPD; art. 28 cpv. 2 CC). D'altro canto, tanto più i dati sono rilevanti per la personalità, maggiore peso acquisirà l'esigenza della persona interessata di ottenere tale cancellazione, anche se è stata lei stessa a pubblicare i dati in un momento precedente. Tale cancellazione potrebbe però essere in contrasto con la salvaguardia dell'interesse della collettività in materia d'informazione, e segnatamente nel caso in cui il soggetto interessato sia una persona di assoluto o relativo rilievo storico[88] o un pubblico ufficiale. Trascorso un certo periodo di tempo il diritto all'oblio può tornare a essere legittimo anche per queste persone[89]. Se a dover essere cancellati sono dati personali pubblicati quando il soggetto era ancora minorenne, considerate la particolare necessità di protezione e, per una certa parte, la limitata capacità d'intendere dei minori, in regola di massima la cancellazione esigerà tempi di reazione molto più tempestivi quando è la personalità di un fanciullo a essere minacciata rispetto a quando si tratta di un adulto.

Un altro problema da ricondurre al diritto all'oblio è il lascito digitale, ossia il trattamento dei dati lasciati su Internet dalle persone decedute. Il diritto successorio, il diritto delle persone e il diritto alla protezione dei dati offrono a questo proposito solo soluzioni parziali[90].

Dall'analisi emerge che la legislazione vigente garantisce in una certa misura il diritto all'oblio, nel complesso limitandone però la portata in presenza di interessi contrastanti, sostenuti da ragionevoli motivazioni (ad es. informazione a beneficio della collettività, proporzionalità delle misure imposte a un gestore di piattaforma ecc.)[91].

Nonostante siano disponibili rimedi giuridici che permettono di eliminare determinati contenuti, dal punto di vista tecnico si può rivelare estremamente complicato ottenerne la completa cancellazione nelle reti sociali. Questo problema diventa ancora più acuto se i suddetti contenuti sono già stati scaricati o riutilizzati da un esteso numero di terzi.

Nel rapporto concernente la valutazione della legge federale sulla protezione dei dati il Consiglio federale considera di precisare il diritto all'oblio.[92]

4.3.4 Reperibilità dei dati nei profili utente sui motori di ricerca

4.3.4.1 Situazione iniziale

Tramite metadati integrati nelle pagine Internet, il crawler dei motori di ricerca può essere indotto a escludere determinati contenuti e pagine dal proprio indice o memoria cache. I gestori di reti sociali possono configurare di conseguenza l'accesso dei motori di ricerca ai dati degli utenti. Il problema

---

[88] Sportivi, politici, artisti, personalità di spicco dell'economia e della società in generale sono persone di assoluto rilievo storico; le persone di relativo rilievo storico sono persone che attirano l'interesse del pubblico in occasione di un evento specifico. *BSK-ZGB I*, Meili Andreas, 4 ed., Basilea 2010, art. 28, pag. 271 n. marg. 52.

[89] Si veda ad es. DTF 109 II 353 consid. 3 e *BSK-ZGB I*, Meili Andreas, 4 ed., Basilea 2010, art. 28, pag. 271 n. marg. 52.

[90] Si rimanda in dettaglio a «Studer Melanie/Schweizer Matthias/Brucker-Kley Elke, Sterben und Erben in der digitalen Welt», in: *Jusletter* 17.12.2012.

[91] Secondo la giurisprudenza della Corte europea dei diritti dell'uomo, la Corte EDU non dà alla persona interessata alcun diritto alla cancellazione di pubblicazioni illegittime apparse sui mezzi di comunicazione archiviati online. Non è compito della giustizia eliminare tutte le tracce di pubblicazioni illecite: Sentenza Corte EDU «Wegrzynowski & Smolczewski c. Polen» (ricorso n. 33846/07) del 16.7.2013, n. 65

[92] Rapporto del Consiglio federale concernente la valutazione della legge federale sulla protezione dei dati del 9 dicembre 2011, cfr. punto 5.2.2 (FF **2012** 239)

sorge in quelle reti sociali che privano l'utente della facoltà di decidere se i dati da loro messi a disposizione delle reti sociali possano essere reperibili su motori di ricerca interni o esterni.

4.3.4.2 Soluzioni adottate all'estero o nel diritto internazionale

La raccomandazione del Consiglio d'Europa per la protezione dei diritti dell'uomo nell'ambito dei motori di ricerca[93] esige che l'utente abbia la facoltà di richiedere al gestore del motore di ricerca di cancellare immediatamente i propri dati personali nel caso in cui questi continuino a essere memorizzati dai motori di ricerca in copie delle pagine Internet originali già rimosse. Inoltre gli utenti dovrebbero poter esigere dall'esercente del motore di ricerca la cancellazione e la correzione dei propri dati che sono stati elaborati. La raccomandazione del Consiglio d'Europa sulla protezione dei diritti dell'uomo nelle reti sociali richiede che gli utenti possano essere informati prima di decidere in merito all'indicizzazione dei loro dati e abbiano il diritto di rimuoverli dalla memoria cache dei motori di ricerca.

Anche il progetto di modifica della legge tedesca sui mezzi di telecomunicazione esige che i conti degli utenti e i contenuti creati da questi siano reperibili da un motore di ricerca esterno soltanto a condizione che l'utente abbia acconsentito in precedenza[94].

4.3.4.3 Situazione legale in Svizzera

Se le reti sociali permettono l'accesso dei motori di ricerca ai dati personali dei membri della rete, vi è una comunicazione di dati ai sensi della legge sulla protezione dei dati (art. 3 lett. e e f LPD) a cui sono applicabili i principi del trattamento dei dati. Il principio della riconoscibilità della raccolta di dati personali (art. 4 cpv. 4 LPD) garantisce alla persona interessata il diritto di essere informato sul fatto che i propri dati personali pubblicati nella rete sociale sono accessibili ai motori di ricerca, a meno che ciò non risulti evidente dalle circostanze.

Se si tiene conto della moltitudine di dati pubblicati nelle reti sociali e del loro carattere spesso molto personale, si presume che molte volte si tratti di dati personali o profili della personalità degni di particolare protezione. Nella maggior parte dei casi, a causa della mancanza di altri motivi giustificativi (art. 13 cpv. 1 LPD), è di conseguenza necessario richiedere un consenso esplicito (art. 4 cpv. 5 LPD) per l'accesso del motore di ricerca ai dati degli utenti. Dal principio dell'uso vincolato dei dati deriva che terzi – in questo caso i gestori dei motori di ricerca –devono attenersi in linea di massima anche alla finalità del trattamento dei dati dichiarata al momento della loro raccolta[95].

Se i gestori dei motori di ricerca eludono le limitazioni all'accesso dati degli utenti che i gestori di reti sociali pongono ai crawler, se comunque raccolgono questi dati e li rendono accessibili al pubblico, a causa della segretezza[96] della loro raccolta tale modo di agire è eventualmente da considerarsi illecito (art. 4 cpv. 1 LPD).

4.3.5 Problemi legati al riconoscimento dell'immagine

4.3.5.1 Situazione iniziale

Le foto caricate su reti sociali che mostrano persone riconoscibili assieme ai rispettivi profili d'utente possono servire allo sviluppo e al miglioramento dei programmi di riconoscimento facciale. Questi strumenti sono in grado di confrontare le persone che compaiono su foto successivamente pubblicate con i dati raccolti e associarle a un profilo utente. Se terzi caricano foto raffiguranti altri membri della rete sociale su una piattaforma, un tale programma può suggerire l'associazione tra la persona sulla

---

[93] Raccommandation CM/Rec(2012)3 sur la protection des droits de l'homme dans le contexte des moteurs de recherche.

[94] Gesetzesentwurf Änderung Telemediengesetz (Progetto di modifica della legge sui mezzi di telecomunicazione), 17/6765.

[95] Rosenthal David /Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 95 n. 47.

[96] La raccolta di dati segreta viola in linea di massima il principio della buona fede e della riconoscibilità del trattamento dei dati (art. 4 cpv. 2 e 4 LPD).

foto e un profilo registrato (*tag-suggest* – suggerimento automatico dei tag)[97]. Inoltre tale programma di riconoscimento facciale può identificare persone interessate a rimanere anonime (per es. su *dating website* – siti d'incontri) o grazie alla foto sulla piattaforma sociale e al nome associatovi può rinviare al curriculum vitae della persona in questione sulla pagina di un'impresa.

Nella stessa direzione evolve il riconoscimento automatico di altre informazioni contenute nelle foto in base ai contorni, ai colori e alla struttura della superficie degli oggetti visualizzati (*content based image retrieval* – CBIR riconoscimento basato sull'immagine). La funzione può identificare edifici o oggetti specifici e probabilmente permettere di localizzare geograficamente la situazione presentata nella foto. Le possibili conseguenze sono la pubblicazione di indirizzi, lo *stalking* (atti persecutori) o altri atti lesivi o illegali.

4.3.5.2 Soluzioni adottate all'estero o nel diritto internazionale

In adempimento alle richieste dell'incaricato della protezione dei dati irlandese, Facebook ha disattivato il proprio programma di riconoscimento facciale nell'Unione europea[98]. Il compromesso ha rappresentato il risultato parziale di un esame generale riguardo alla conciliabilità dei servizi dell'impresa con il diritto sulla protezione dei dati dell'Irlanda e dell'Unione europea. Secondo l'IFPDT l'accordo vale anche per la Svizzera.

La raccomandazione del Consiglio d'Europa sulla protezione dei diritti dell'uomo nelle reti sociali esige che le tecnologie che hanno un influsso determinante sulla sfera privata degli utenti (in quanto basate per esempio sul trattamento di dati sensibili o biometrici, come appunto i programmi di riconoscimento facciale) garantiscano un'elevata protezione dei dati e che queste non siano utilizzate senza il consenso degli utenti.

Nel suo parere relativo al riconoscimento facciale nell'ambito dei servizi online e mobili[99], il gruppo di lavoro articolo 29 per la protezione dei dati, un organo consultivo indipendente della Commissione europea, si è occupato dei rischi in materia di legislazione sulla protezione dei dati legati a questa tecnologia e ha emanato raccomandazioni per chi tratta i dati che riguardano l'ottenimento di un valido consenso della persona interessata, il criptaggio dei dati trasmessi e la loro conservazione sicura.

4.3.5.3 Situazione legale in Svizzera

Affinché il programma di riconoscimento facciale possa essere utilizzato nelle reti sociali, devono essere dapprima pubblicate delle immagini su una piattaforma. Quale contenuto parziale dell'articolo 28 capoverso 1 CC il diritto alla propria immagine protegge il singolo individuo dall'uso illecito della propria immagine[100]. Se non si ottiene un consenso in precedenza o successivamente, di norma nessuno può essere raffigurato e immagini già esistenti non possono essere pubblicate; inoltre il consenso dato per prendere una foto non comprende ogni possibile pubblicazione successiva bensì, in linea di massima, unicamente quella che appare chiaramente alla persona interessata al momento dello scatto dell'immagine[101].

---

[97] La persona A per esempio esamina le foto prese dalla persona B con un programma di riconoscimento facciale, riconosce la persona C e ne indica il nome sulla sua foto.

[98] Report of Re-Audit Facebook Ireland Ltd of the Data Protection Commissioner from 21.09.2012; consultabile su: http://dataprotection.ie/viewdoc.asp?DocID=1233&m=f; Driessen Benedikt / Dürmuth Markus, "Anonymität und Gesichtserkennung", in: *digma* 2013, pag. 54.

[99] Parere del Gruppo di lavoro articolo 29 per la protezione dei dati 00727/12/IT WP 192.

[100] Bächli Marc, *Das Recht am eigenen Bild*, Basilea 2002, pag. 69.

[101] A meno che non esista una valida giustificazione ai sensi dell'art. 28 cpv. 2 CC. Un limite è posto al diritto alla propria immagine per esempio da interessi di pubblicazione giustificati (libertà d'espressione ai sensi dell'art. 10 CEDU); cfr. in merito alla giurisprudenza di Strasburgo Zeller Franz, "Das eigene Bild und sein begrenzter Schutz", in: *digma* 2013/2, pag. 50 segg.

Anche il diritto sulla protezione dei dati, le cui disposizioni di diritto privato completano e concretizzano la protezione della personalità in generale[102], vieta che l'immagine di una persona[103] sia pubblicata a sua insaputa. Il principio della riconoscibilità della raccolta dei dati (art. 4 cpv. 4 LPD) esige che per le persone raffigurate appaia evidente almeno dalle circostanze se le immagini su di loro saranno pubblicate nelle reti sociali. Inoltre il principio dell'uso vincolato dei dati garantisce che i dati personali siano trattati soltanto per lo scopo stabilito al momento della loro raccolta. La pubblicazione di foto di una persona nelle reti sociali è pertanto permessa, senza un motivo giustificativo (art. 13 cpv. 1 LPD), unicamente se al momento dello scatto dell'immagine risultava evidente che essa fosse destinata alla pubblicazione su una rete.

Se sono state pubblicate delle foto di persone nelle reti sociali, allora la loro analisi e associazione a profili utente tramite un programma di riconoscimento facciale sono permesse unicamente se le persone interessate sono state informate di questo tipo di utilizzazione[104], il che non è affatto il caso per quelle foto pubblicate da terzi senza il consenso della persona interessata. Le foto devono essere regolarmente considerate dati personali degni di protezione particolare (art. 3 cpv. c LPD), il che pone di conseguenza elevati requisiti in materia di protezione dei dati[105]. Di principio l'impiego di un programma di riconoscimento facciale automatico assieme alla funzione del *tag suggest* (suggerimento automatico dei tag) viola anche il principio della proporzionalità del trattamento dei dati (art. 4 cpv. 2 LPD).

Di dubbia interpretazione è il caso in cui una persona abbia pubblicato le proprie foto consapevolmente e volontariamente nella rete sociale e reso il proprio profilo accessibile a tutti tramite le impostazioni utente (art. 12 cpv. 3 LPD). Se i dati personali resi pubblicamente accessibili vengono trattati per finalità che al momento della pubblicazione non erano oggettivamente riconoscibili dalle circostanze, si commette egualmente una lesione della personalità[106]. Tenuto conto della relativa novità dell'impiego di un programma di riconoscimento facciale, si può dubitare del fatto che, se una persona rende le proprie foto accessibili a tutti, lo faccia anche al fine di un tale trattamento dei dati. Anche in questo caso si dovrebbe verificare se sia presente un consenso per il concreto trattamento dei dati[107].

Per quanto concerne il riconoscimento automatico di caratteristiche e oggetti sulle immagini da parte di un programma informatico, tali informazioni devono essere considerate quali dati relativi a oggetti. Se possono essere associati a una persona, si qualificano sempre quali dati personali ai sensi della legge sulla protezione dei dati. A titolo esemplificativo, si considerino appezzamenti di terreno o veicoli a motore[108]. In questo caso anche questi beneficiano della protezione della legge sulla protezione dei dati.

4.3.6 Problemi di geolocalizzazione (tecnologia di localizzazione)

4.3.6.1 Situazione iniziale

Certe reti sociali offrono servizi che situano gli utenti (i cui dati sono di solito trasmessi tramite *smartphones* – telefonini intelligenti) avvalendosi di tecnologie di localizzazione come il GPS o la WLAN e forniscono su richiesta informazioni relative alla località in questione. Certe reti sociali si specializzano addirittura unicamente in questi servizi di geolocalizzazione[109]. A seconda del comportamento di co-

---

[102] Schweizer Michael, *Recht am Wort*, Berna 2012, pag. 209.

[103] Rientrano nel concetto di dati personali della legge sulla protezione dei dati anche immagini di persone a condizione che queste possano essere associate a una persona; pertanto sono incluse anche le fotografie.

[104] Ciò deriva dalle esigenze di ottenere un consenso secondo l'art. 28 cpv. 2 CC e art. 13 cpv. 1 LPD nonché dai principi della buona fede e dell'uso vincolato del trattamento dei dati ai sensi dell'art. 4 cpv. 2 e 3 LPD.

[105] Vedi art. 4 cpv. 5, art. 11a cpv. 3 lett. a, art. 12 cpv. 2 lett. c nonché art. 14 LPD.

[106] Rosenthal David/Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 381 n. 76.

[107] Rosenthal David/Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 383 n. 84.

[108] *BSK-DSG*, Belser Urs, 2ª ed., Basilea 2006, art. 3, pag. 64 n. marg. 5. Ai sensi anche della DTF 138 II 346 consid. 6.2.

[109] Si veda anche Foursquare (https://foursquare.com/), o anche Friendticker (http://en.friendticker.com/) .

municazione degli utenti, i gestori della piattaforma possono associare una grande quantità di dati ai geodati rilevati. In questo modo non soltanto conoscono la posizione approssimata dell'utente, ma possono risalire persino all'edificio (per es.: cinema, ristorante, ecc.), sapere con chi è, cosa sta facendo e se è di suo gradimento.

La connessione di tali servizi di localizzazione con le reti sociali può indurre gli utenti a comunicare consapevolmente o inconsapevolmente informazioni in merito al luogo in cui si trovano e alle attività che vi svolgono, informazioni che persone esterne possono utilizzare per fini non previsti dall'utente. Comportamenti lesivi come il furto d'identità, il mobbing su Internet, atti persecutori su Internet o il *cybergrooming* (l'adescamento di minori su Internet) possono essere agevolati da tali tecnologie. Inoltre i dati relativi alle località possono svelare a terzi dove si trovano le persone interessate e dove queste abitano e così facilitare i furti[110].

4.3.6.2 Soluzioni adottate all'estero o nel diritto internazionale

Nel suo parere del maggio 2011 il gruppo di lavoro art. 29 della protezione dei dati[111] si è occupato dei rischi legati ai servizi di geolocalizzazione che incombono sulla legislazione in materia di protezione dei dati[112]. La questione centrale è il consenso degli utenti che, secondo il parere, non è valido se si basa sull'accettazione obbligatoria delle condizioni commerciali generali o se vi è unicamente la possibilità dell'*opt-out* (opzione di esclusione). I servizi di geolocalizzazione dovrebbero in linea di massima essere disattivati e prevedere la possibilità di *opt-in* (opzione di adesione) per gli utenti. Si dovrebbe esplicitamente richiamare l'attenzione degli utenti in merito a finalità di trattamento dei dati inconsuete, quali per esempio la creazione di profili utente o il ricorso al *behavioural targeting* (pubblicità orientata al comportamento degli utenti). Se gli utenti vengono informati in merito a modifiche della finalità del trattamento o alla trasmissione dei dati, allora il loro silenzio non può essere interpretato quale consenso tacito. Il dispositivo terminale dovrebbe segnalare all'utente tramite un simbolo d'avvertimento qualora sia in funzione un servizio di geolocalizzazione e di norma i fornitori di servizi dovrebbero richiedere sistematicamente il consenso dell'utente anche senza alcuna modifica della prestazione. Anche il periodo di conservazione dei dati dovrebbe, a tal fine, essere a breve termine e gli utenti dovrebbero avere il diritto di essere informati in formato leggibile nonché disporre della facoltà di modificare e cancellare i propri dati.

4.3.6.3 Situazione legale in Svizzera

I geodati costituiscono dati personali ai sensi della legislazione sulla protezione dei dati se sussiste una connessione con una persona fisica o giuridica o se una possibile connessione può essere ottenuta con un dispendio di tempo ragionevole[113]. Attraverso la localizzazione di dispositivi terminali mobili associati a persone e la correlazione di dati concernenti oggetti e persone si possono inoltre generare profili di personalità o dati personali degni di particolare protezione[114], il trattamento dei quali è rigorosamente disciplinato nella legge sulla protezione dei dati. A livello legislativo, i rischi derivanti dai servizi di geolocalizzazione delle reti sociali sono in linea di massima contemplati nei principi del trattamento dei dati nella legge sulla protezione dei dati.

Così per esempio, se vengono raccolti e associati più dati rispetto a quanto sia necessario alla finalità del loro trattamento, si applica il *principio della proporzionalità del trattamento dei dati* (art. 4 cpv. 2 LPD). Tale principio potrebbe addirittura determinare l'anonimità dei dati geocodificati[115].

---

[110] Hilty/Oertel/Wölk/Pärli, *Lokalisiert und identifiziert*, Zurigo 2012, pag. 162seg.

[111] https://secure.edps.europa.eu/EDPSWEB/edps/lang/fr/Cooperation/Art29

[112] Avis 13/2011 sur les services de géolocalisation des dispositifs mobiles intelligents du 16.05.2011, 881/11/FR WP 185.

[113] FF **2006** 7200 seg.

[114] Hilty/Oertel/Wölk/Pärli, *Lokalisiert und identifiziert*, Zurigo 2012, pag. 48 seg., 55 seg.

[115] Hilty/Oertel/Wölk/Pärli, *Lokalisiert und identifiziert*, Zurigo 2012, pag. 47.

Il *principio dell'uso vincolato dei dati* (art. 4 cpv. 3 LPD) contempla la rettifica della finalità del trattamento dei dati, se il gestore della piattaforma utilizza a posteriori i dati personali rilevati in base alla loro utilità per nuove finalità. Generare dati personali usuali, profili della personalità o dati personali degni di particolare protezione tramite l'associazione a geodati o ad altri dati pubblicati nelle reti sociali devono essere azioni riconoscibili per le persone interessate[116] e i gestori delle reti sociali devono evitare la creazione, per quanto possibile, di dati errati al momento della loro associazione (art. 5 cpv. 2 LPD).

Come succede in molti servizi offerti dalle reti sociali, anche in questo caso all'utente sono sovente fornite delucidazioni carenti in merito all'estensione, alla trasmissione, al tipo e alla finalità del trattamento dei dati legati alla propria localizzazione, a cui possono aggiungersi anche dubbi in merito all'efficacia e alla validità del relativo *consenso*[117].

L'articolo 45*b* della legge sulle telecomunicazioni (LTC) disciplina la geolocalizzazione per i clienti di fornitori di servizi di telecomunicazione. È autorizzata in tre casi: nel primo caso se l'ubicazione è necessaria per i servizi di telecomunicazione o per la loro fatturazione, nel secondo caso se i clienti hanno dato il loro consenso e nel terzo caso se i dati sono resi anonimi. La maggior parte degli operatori di media sociali digitali non sono però allo stesso tempo fornitori di servizi di telecomunicazione (vedi sopra punto 2.4.2.2*), cosicché l'articolo 45*b* spesso non è applicabile.

4.3.7 Legame eccessivo dell'utente alla rete sociale

4.3.7.1 Situazione iniziale

Nelle scienze economiche si parla di effetto di *lock in* quando per un'impresa è particolarmente difficile slegarsi da una collaborazione con un'impresa partner in cui sono stati effettuati importanti investimenti. L'impresa partner può sfruttare la situazione per dettare condizioni particolarmente sfavorevoli.

Gli utenti delle reti sociali possono trovarsi in una situazione simile se hanno investito così tanto tempo e fatica per presentarsi su una piattaforma sociale da non poter concepire un cambiamento. Allora la piattaforma può modificare le condizioni a svantaggio degli utenti senza che questi ultimi reagiscano e passino a una piattaforma della concorrenza.

Questo è il caso per esempio se immagini, film, musica e testi importanti e altri dati degli utenti sono memorizzati sulla piattaforma. È anche possibile che gli utenti siano in contatto con talmente tante persone tramite una piattaforma (per esempio tramite il proprio canale YouTube personale o un blog) che passerebbero a un'altra piattaforma soltanto a patto di potervi trasferire questi contatti.

Un cambiamento della piattaforma può sembrare altrettanto impensabile se gli utenti possono scambiare tra di loro messaggi unicamente tramite la piattaforma, in mancanza della quale perderebbero la possibilità di contattarsi. D'altra parte in questo caso può essere anche l'intenzione degli altri utenti di poter essere contattati soltanto tramite la piattaforma, rimanendo così nell'anonimato, e per esempio di non rivelare il proprio indirizzo e-mail al gestore della piattaforma. La possibilità di contattarsi tramite un'altra piattaforma non costituisce un'opzione confacente agli interessi di tali utenti. Una risposta a questo conflitto d'interessi può essere quella di conservare il contatto con gli utenti che lo desiderano anche al di fuori della piattaforma.

Alcune piattaforme offrono agli utenti la possibilità di prendere con sé i dati memorizzati. In linea di massima si dovrebbe permettere la portabilità dei dati tra diverse piattaforme in quanto solo in questo modo diminuirebbe a un livello ammissibile l'onere di lavoro legato al cambiamento di una piattaforma.

---

[116] Qui intervengono i principi della buona fede e della riconoscibilità del trattamento dei dati nonché l'obbligo d'informazione del detentore di una collezione di dati per la raccolta di profili di personalità o di dati personali degni di particolare protezione (art. 4 cpv. 2 e 4 nonché art. 14 LPD).

[117] Hilty/Oertel/Wölk/Pärli, *Lokalisiert und identifiziert*, Zurigo 2012, pag. 65.

4.3.7.2 Soluzioni adottate all'estero o nel diritto internazionale

La raccomandazione del Consiglio d'Europa relativa alle reti sociali esige una semplice portabilità dei dati a un altro fornitore tramite un formato elettronico di uso comune.

Anche la proposta UE di regolamento sulla protezione dei dati prevede il diritto alla portabilità dei dati[118]. L'interessato ha il diritto, ove i dati personali siano trattati con mezzi elettronici e in un formato strutturato e di uso comune, di ottenere dal responsabile del trattamento copia dei dati trattati in un formato elettronico e strutturato che sia di uso comune e gli consenta di farne ulteriore uso. Se ha fornito i dati personali, l'interessato ha il diritto di trasmettere tali dati personali a un altro sistema in un formato elettronico di uso comune, senza impedimenti da parte del responsabile del trattamento da cui sono richiamati i dati.

4.3.7.3 Situazione legale in Svizzera

Nel diritto svizzero non esiste alcuna norma che obblighi le reti sociali a consegnare ai propri utenti, una volta che abbandonano la piattaforma, quei dati che vi sono stati pubblicati e memorizzati. Una tale norma potrebbe rivelarsi efficace contro un eccessivo legame degli utenti a determinate piattaforme.

Un obiettivo comparabile è fissato nella vigente regolamentazione della portabilità dei numeri contemplato nella legislazione sulle telecomunicazioni. Questa permette alla clientela di mantenere il proprio numero telefonico qualora cambino il fornitore del servizio telefonico o l'indirizzo. Chi cambia fornitore può conservare il proprio numero telefonico presso il nuovo fornitore e risparmiarsi la fatica di comunicare a tutti i propri contatti il nuovo numero telefonico. Ciò facilita pertanto il passaggio a un nuovo fornitore.

Il mercato delle reti sociali è tuttavia ancora troppo in fermento. Il legame dell'utente a una determinata piattaforma non è, esattamente per questo motivo, ancora così marcato come lo sarebbe in un mercato consolidato. Solo una volta stabilizzatosi, il mercato la fidelizzazione della clientela esistente assumerà un ruolo più importante per l'impresa. È prevedibile che, per scoraggiare la clientela esistente dal cambiare piattaforma, le imprese non acconsentiranno a fornire loro i dati. Nella prassi oggigiorno si rileva che è già possibile prendere con sé molti dati registrati nelle reti sociali più diffuse. A fronte delle offerte spontanee esistenti, al momento un obbligo particolare per il rilascio dei dati non risulta ancora essere necessario. Questa ragione è altresì avvalorata dalle questioni che l'attuazione di un tale obbligo solleverebbe: ciò lo confermano a maggior ragione anche le domande che verrebbero a porsi all'attuazione di quest'obbligo: quali dati può prendere con sé l'utente? Anche dati che il gestore ha associato ad altri dati per renderli più utili (per es. l'indicazione dell'utente sulle foto pubblicate da altrui)? Anche i dati che sono stati creati tramite i programmi del gestore? Quali dati e in quale formato devono essere rilasciati?

Come si evolverà tale tema in futuro non si può ancora prevedere oggi. È pertanto opportuno osservare gli sviluppi futuri ed eventualmente emanare delle prescrizioni legali in un momento successivo (si veda in merito punto **Erreur ! Source du renvoi introuvable.**).

[118] Art. 8 Proposta UE Regolamento generale sulla protezione dei dati, COM(2012) 11 definitivo.

4.4 Pregiudizio degli interessi individuali cagionato da terzi

4.4.1 Delitti contro l'onore e lesioni della personalità illecite

4.4.1.1 Situazione iniziale

Anche nelle reti sociali compaiono giudizi lesivi dell'onore o false esposizioni di fatti[119]. In Svizzera sono già state pronunciate sentenze a causa di ingiurie nelle reti sociali [120]. Ledere la reputazione attraverso i media sociali non è paragonabile a semplici lesioni dell'onore perpetrate con i tradizionali mezzi di comunicazione (per esempio nei giornali). All'estero è stato riconosciuto che la comunicazione online tramite nuovi canali come i blog o Twitter mette a dura prova l'efficacia degli strumenti giuridici esistenti per la tutela della reputazione.[121]

Per le persone interessate sono insorti nuovi rischi, difficili da calcolare. Così in molte reti sociali i contenuti possono essere inseriti sui profili di utenti terzi senza precedentemente richiederne il consenso, il che rende più difficile controllare il proprio profilo. Data la trasmissione semplice, istantanea e non verificata di contenuti nelle reti sociali e la rilevanza sociale dei gruppi di contatti spesso notevole per gli utenti, il danno arrecato da terzi a causa di giudizi di valore lesivo al proprio onore o esposizioni di fatti false può essere ingente.

Un altro fenomeno che può nuocere alla buona reputazione della persona interessata è rappresentato per esempio dagli inviti a gruppi su Facebook. Se un terzo viene invitato da un amico su Facebook a iscriversi a un gruppo, ne diviene automaticamente membro indipendentemente dal fatto che abbia espresso il suo consenso o meno. Questi viene immediatamente informato dell'invito e può uscire subito dal gruppo. Fino a questo momento, a seconda del profilo del gruppo e dell'identità della persona invitata, può già essere stata danneggiata la sua reputazione.

4.4.1.2 Soluzioni adottate all'estero o nel diritto internazionale

Una possibile misura per la protezione contro pubbliche esposizioni di fatti errate è il diritto di rettifica. Secondo la raccomandazione del Consiglio europeo sul diritto di rettifica nel nuovo ambito dei media[122] tale diritto dovrebbe essere applicabile a tutti i mezzi di comunicazione che servono a trasmettere regolarmente al pubblico contenuti controllati sul piano redazionale, indipendentemente dal fatto che siano pubblicati su Internet o meno. Se contenuti dibattuti rimangono pubblicamente accessibili negli archivi elettronici ed è stato garantito il diritto di rettifica, allora tramite un *link* (collegamento ipertestuale) si dovrebbe rinviare ai contenuti della rettifica.

Il Parlamento europeo e il Consiglio d'Europa hanno sollecitato gli Stati membri a disporre misure per garantire il diritto di rettifica nei mezzi di comunicazione in linea[123]. Nella sua relazione in merito all'attuazione della raccomandazione del 2011 la Commissione europea riteneva che l'introduzione di un

---

[119] Nel rapporto annuale 2011 lo SCOCI registra una crescita delle segnalazioni di delitti contro l'onore e constata che sempre più atti criminali sono perpetrati mediante le reti sociali. Cfr. Rapporto annuale 2011 Servizio di coordinazione per la lotta contro la criminalità su Internet SCOCI, pag. 6.

[120] Cfr. la decisione del Tribunale di circolo di San Gallo del 9.5.2011 (Ingiurie via Facebook); http://wifimaku.com/pages/viewpage.action?pageId=5669650

[121] Tratto dalla più recente letteratura estera cfr. per esempio Ladeur Karl-Heinz/Gostomzyk Tobias, «Der Schutz von Persönlichkeitsrechten gegen Meinungsäusserungen in Blogs», *Neue Juristische Wochenschrift NJW* 2012, pag. 710 segg.; Richardson Megan, «Honour in a Time of Twitter», *Journal of Media Law* 2013, pag. 45 segg.

[122] Recommandation Rec(2004)16 sur le droit de réponse dans le nouvel environnement des médias.

[123] Raccomandazione del Parlamento europeo e del Consiglio del 20 dicembre 2006 relativa alla tutela dei minori e della dignità umana e al diritto di rettifica relativamente alla competitività dell'industria europea dei servizi audiovisivi e d'informazione in linea, GU L 378 del 27.12.2006, pag. 72.

diritto di rettifica in relazione ai mezzi di comunicazione in linea negli Stati membri fosse molto incoerente[124], e invitava a migliorare l'efficacia dei sistemi.

4.4.1.3 Situazione legale in Svizzera

La tutela dell'onore nel Codice penale (art. 173-178 CP) e nel Codice civile (art. 28 seg. CC) è in linea di massima applicabile anche alle attività nelle reti sociali. La tutela dell'onore sul piano economico di cui all'art. 28 CC viene completata dall'articolo 3 capoverso 1 lettera a LCSI.

Quale strumento particolare il CP ricorre al diritto di risposta in relazione all'esposizione di fatti su mezzi di comunicazione sociale di carattere periodico che si rivolgano o sono accessibili al pubblico (art. 28*g* – 28l CP). Il legislatore ha espressamente formulato il concetto di mezzi di comunicazione in modo generico così che il diritto di risposta trova applicazione anche a nuove forme dei mezzi di comunicazione e non dipende dalla tecnologia impiegata per la diffusione[125]. L'utilizzo effettivo della rispettiva piattaforma o il comportamento del titolare del profilo nel pubblicare contenuti determinano la qualifica dei profili utente delle reti sociali come mezzi di comunicazione di carattere periodico. In tal senso i blog di giornalisti aggiornati regolarmente possono essere considerati senza dubbio mezzi di comunicazione di carattere periodico ai sensi del CP, mentre ciò resta dubbio nel caso dei forum di discussione[126].

Problemi pratici nel procedere contro contenuti infamanti e lesivi della personalità nelle reti sociali si riscontrano innanzitutto a livello esecutivo, nel caso in cui l'autore della lesione dell'onore non sia identificabile e le indagini dipendano dalla volontà di cooperazione dei gestori delle piattaforme e dai fornitori di servizi Internet. Particolarmente difficile è intervenire velocemente contro pubblicazioni apparse su piattaforme estere.[127] (Nel caso di compartecipanti svizzeri l'attuazione della legge è invece agevolata dal fatto che le domande di cessazione e di constatazione possano essere fatte valere contro tutte le persone che commettono una lesione della personalità).[128])

Gli strumenti giuridici perdono in gran parte d'efficacia se i contenuti lesivi si sono diffusi a velocità ed estensione incontrollabili: anche chi ha affermato con successo i propri diritti della personalità in tribunale, deve tenere in conto che il contenuto illegale riapparirà altrove[129].

4.4.2 Bullismo su Internet e stalking su Internet

4.4.2.1 Situazione iniziale

Una particolare forma di lesione della personalità è il bullismo su Internet o il mobbing su Internet[130], vale a dire la diffusione di testi, immagini o film diffamatori tramite l'uso di moderni mezzi di comunicazione (cellulare, chat, reti sociali, portali video, forum di discussione o blog), con cui si denigra, offen-

---

[124] Relazione della Commissione sull'applicazione della raccomandazione del Consiglio, del 24 settembre 1998, concernente la tutela dei minori e della dignità umana e della raccomandazione del Parlamento europeo e del Consiglio, del 20 dicembre 2006, relativa alla tutela dei minori e della dignità umana e al diritto di rettifica relativamente alla competitività dell'industria europea dei servizi audiovisivi e d'informazione in linea – Tutela dei minori nel mondo digitale –, COM(2011) 556 definitivo, pag. 10.

[125] DTF 113 II 369 consid. 3 pag. 371.

[126] Cfr. per es. Barrelet Denis/ Werly Stéphane, *Droit de la communication*, Berna 2011, n. 1683.

[127] Si veda in tal senso Schneider-Marfels Karl-Jascha, *Facebook, Twitter & Co: "Imperium in imperio"*, in: Jusletter del 20 febbraio 2012.

[128] Cfr. per esempio la sentenza in merito a una piattaforma blog gestita dalla Tribune de Genève (TF 5A_792/2011 del 14.1.2013).

[129] Ladeur Karl-Heinz/Gostomzyk Tobias, *Der Schutz von Persönlichkeitsrechten gegen Meinungsäusserungen in Blogs*, Neue Juristische Wochenschrift NJW 2012, pag. 713.

[130] In questo rapporto questi due termini sono sinonimi.

de o molesta una determinata persona[131]. Solitamente queste aggressioni si ripetono nel tempo o persistono durante un periodo prolungato[132].

Lo *stalking* (atti persecutori su Internet) indica l'uso di mezzi di comunicazione elettronici, come per esempio le reti sociali digitali, per opprimere terzi. Con l'espressione *atti persecutori su Internet* si intendono la persecuzione e la molestia reiterate di una persona. Questa forma di violenza si può manifestare sotto forma di osservazione, controllo o contatto. Spesso si verificano atti persecutori su Internet tra persone che si conoscono già o che sono prossime. I dati messi a disposizione sulle reti sociali dall'utente stesso possono essere utilizzati, oltre che per molestie su Internet, anche per scoprire l'indirizzo delle potenziali vittime, studiare le loro abitudini e perseguitarle al di fuori di Internet in modo fisico.

Il fenomeno del bullismo su Internet e degli atti persecutori su Internet non si limitano alle reti sociali ma occorrono sempre di più anche in questo contesto, in presenza di particolari circostanze[133]. La possibilità di presentarsi nelle reti sociali con uno pseudonimo permette agli aggressori di agire nell'anonimato, il che facilita la molestia e l'avvilimento di terzi. Questi atti lesivi possono essere inoltre commessi nelle reti sociali in modo tale che siano visibili anche per persone esterne, il che aggrava il danno arrecato alla vittima.

4.4.2.2 Soluzioni adottate all'estero o nel diritto internazionale

La raccomandazione del Consiglio d'Europa sulla protezione dei diritti dell'uomo nelle reti sociali invita allo scambio della buona prassi in merito alla prevenzione contro il bullismo su Internet (e l'adescamento di minori su Internet). Inoltre i gestori delle piattaforme dovranno mettere a disposizione efficaci meccanismi per inoltrare reclami e trattare quelli trasmessi in modo accurato.

La campagna di sensibilizzazione «klicksafe» condotta su mandato della Commissione europea per promuovere le competenze mediatiche nell'utilizzo di Internet e dei nuovi media informa tra l'altro su Internet anche sui fenomeni del mobbing e del bullismo su Internet, delucida il diritto vigente e dà dei consigli generali agli interessati su come procedere in modo appropriato[134].

La Corea del Sud ha cercato di combattere i gravi casi di bullismo su Internet e di portare avanti l'idea di correttezza in relazione alle elezioni politiche[135] introducendo un obbligo d'identificazione nelle reti sociali[136]. In seguito alla decisione della corte suprema della Corea del Sud sull'anticostituzionalità

---

[131] In uno studio condotto nei Cantoni Vallese, Turgovia e Ticino tra il novembre del 2010 e il giugno del 2012 con 960 studenti – di cui il 49 per cento di sesso femminile, con un'età media di 13,5 anni – attesta che, seppur il numero di vittime e dei colpevoli del bullismo su Internet sia molto basso, l'incidenza dei casi ha registrato un aumento tra il 2010 e il 2012. Si veda: cifre inedite tratte dallo Studio netTEEN (Perren S. & Sticca F., 2012. Jacobs Center for Productive Youth Development, Università di Zurigo). Inoltre il bullismo su Internet tra i giovani sembra essere di regola strettamente connesso alle forme di bullismo tradizionale, visto che le vittime e i rei nell'ambito Internet nella maggior parte dei casi sono rispettivamente colpiti o attivi anche quando sono *offline* (non in rete). Vedi: Perren Sonja, *Professionswissen für Lehrerinnen und Lehrer – Grundlagen für die Aus- und Weiterbildung von Lehrerinnen und Lehrern*, ed.: H.U. Grunder, K. Kansteiner-Schänzlin, H.Moser, pag. 15.

[132] Rapporto del Consiglio federale del 26.05.2010 *Protezione dal ciberbullismo*; consultabile alla pagina: http://www.ejpd.admin.ch/content/ejpd/it/home/dokumentation/info/2010/ref_2010-06-02.html .

[133] Nel suo rapporto annuale 2011 lo SCOCI ritiene che vi sia una crescita delle segnalazioni in seguito a minaccia e coazione e che queste siano sempre più ricorrenti nelle reti sociali. Nelle categorie "delitti contro l'onore, minaccia e coazione" sono contenuti anche 30 casi di ciberbullismo. Non è però indicato se sia stato fatto ricorso alle reti sociali o alla posta elettronica. (Vedi Rapporto annuale 2011 SCOCI, pag. 6). Secondo una comunicazione interna dello SCOCI in merito al rapporto annuale 2011, nove dei delitti contro l'onore sono stati perpetrati anche tramite o nell'ambito delle reti sociali e tre delitti che rientrano nella categoria "minaccia, coazione, estorsione" sono avvenuti in reti sociali. Quest'aumento significativo non si è tuttavia ripetuto nel 2012, interrompendo, secondo le stime dello SCOCI, l'aumento registrato nei due anni precedenti (rapporto annuale SCOCI 2013, pag. 9).

[134] Si veda http://www.klicksafe.de/themen/kommunizieren/cyber-mobbing/ .

[135] Introduzione di un sistema per l'identificazione forzata delle persone che si esprimono su siti web o forum Internet in favore o contro candidati politici Public Officials Election Act (POEA) nel 2005.

[136] Si rimanda al rapporto del relatore speciale dell'ONU per la promozione e la protezione del diritto alla libertà d'espressione nella Corea del Sud del 21.03.2011, A/HRC/17/27/Add.2 e al rapporto sulla Corea del Sud dell'iniziativa OpenNet; entrambi consultabili alla pagina: http://www.access-controlled.net/profiles/ .

dell'obbligo di svelare la propria identità[137], agli innumerevoli attacchi da parte di pirati informatici sul server dei fornitori dei relativi siti web e al furto di dati personali di milioni di sudcoreani, la Commissione coreana della comunicazione ha deciso di smantellare entro il 2014 il sistema che richiede la verifica dell'identità[138]. L'obbligo di licenza per portali informativi con più di 50 000 utenti è stato introdotto a Singapore nel giugno 2013[139].

4.4.2.3 Situazione legale in Svizzera

La legislazione svizzera non contiene alcuna disposizione specifica per il bullismo su Internet o per le molestie sessuali su Internet. Tuttavia il diritto penale e civile vigenti contemplano molti atti che, se perpetrati tramite mezzi di comunicazione elettronici, possono essere associati a entrambi questi concetti. Nel suo rapporto sul bullismo su Internet il Consiglio federale ritiene che al momento non vi sia alcuna lacuna nel diritto penale esistente[140].

Agli atti associati ai termini *atti persecutori su Internet* e *bullismo su Internet* è applicabile la tutela dell'onore nel diritto penale (art. 173-178 CP) e nel diritto civile (art. 28 seg. CC). Oltre ai diritti di cui all'articolo 28*a* CC, per proteggersi da lesioni della personalità sotto forma di violenza, minacce o insidie, le persone interessate possono far valere presso un tribunale il divieto di essere contattati da terzi – il che comprende esplicitamente la comunicazione elettronica (art. 28*b* cpv. 1 lett. 3 CC).

Garantiscono ulteriore protezione l'articolo 135 (rappresentazione di atti di cruda violenza), 143bis (accesso indebito a un sistema per l'elaborazione di dati), 144bis (danneggiamento di dati), 156 (estorsione), 179^{novies} (sottrazione di dati personali), 180 (minaccia), 181 (coazione), 197 (pornografia) e 198 (molestie sessuali) del codice penale.

Anche qui le maggiori difficoltà si presentano nuovamente a livello esecutivo. La ricerca dell'identità del reo dovrebbe essere agevolata in quanto spesso proveniente dalla cerchia sociale della persona interessata (scuola, luogo di lavoro, ecc.). Nel 2012 lo SCOCI ha registrato un calo di segnalazioni concernenti i delitti contro l'onore. Tale dato potrebbe essere ricondotto alla maggiore attenzione consacrata dai media ai **casi di bullismo su Internet** e alla conseguente sensibilizzazione dei cittadini a un uso maggiormente consapevole dei media sociali digitali [141].

4.4.3 Furto d'identità e altri pericoli derivanti dalla manipolazione malintenzionata

4.4.3.1 Situazione iniziale

In molte reti sociali il *furto d'identità* può essere commesso facilmente. Nell'ambito della criminalità su Internet il furto e l'abuso d'identità sono in aumento nelle reti sociali digitali e sono spesso finalizzate a commettere delitti sul piano del diritto patrimoniale[142]. Inoltre il furto d'identità può servire per danneg-

---

[137] La corte costituzionale della Corea del Sud ha dichiarato anticostituzionale l'obbligo di svelare la propria identità: "South Korea's real-name net law is rejected by court", 23.08.2012; consultabile alla pagina: http://www.bbc.co.uk/news/technology-19357160 .

[138] Si veda pure Kate Jee-Hyung Kim, *Lessons Learned from South Korea's Real-Name Policy*, 17.01.2012, consultabile alla pagina: http://www.koreaittimes.com/story/19361/lessons-learned-south-koreas-real-name-verification-system e *Real-name Internet law on way out*, Korea Joonang Daily, 30.12.2011; consultabile alla pagina: http://koreajoongangdaily.joinsmsn.com/news/article/article.aspx?aid=2946369 .

[139] Cfr. pure NZZ n. 123 del 31.5.2013, pag. 5: Lizenzpflicht für Onlinemedien – Singapur verschärft die Aufsicht über Nachrichtenportale im Internet.

[140] Rapporto del Consiglio federale del 26.05.2010 *Protezione dal Ciberbullismo*. Il Consiglio federale aveva anche respinto l'introduzione di una nuova fattispecie penale sulla violenza psicologica nel mondo del lavoro richiesta nella mozione di Freysinger 10.4054, in quanto il diritto vigente disciplina già ampiamente le azioni in questione e l'introduzione di un'ulteriore norma penale non avrebbe apportato alcun vantaggio ulteriore. Il Collegio ritiene infatti che ciò non risponderebbe ai problemi centrali legati alla dimostrabilità dei fatti e alle difficoltà che insorgono per le persone coinvolte nel perseguire legalmente il comportamento in questione. Si veda http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20104054. Anche il Consiglio nazionale ha respinto l'introduzione di una fattispecie penale sul mobbing con 130 voti contro 33 e 11 astensioni.

[141] Rapporto annuale SCOCI 2012, pag. 9

[142] ENISA Threat Landscape Report del 28.09.2012, pag. 21 segg.; consultabile alla pagina: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape.

giare la reputazione o per altre lesioni della personalità o dell'onore di terzi. Gli utenti creano un profilo con il nome di una persona famosa e approfittano della sua notorietà o la diffamano assumendo un atteggiamento disdicevole. Allo stesso modo possono allestire un profilo a nome di una persona appartenente alla propria sfera personale per danneggiarla, ridicolizzandola o per inviare contenuti illegali o diffamatori firmati a suo nome.

Anche la creazione di un'*identità immaginaria* nelle reti sociali digitali può apportare agli utenti vantaggi di cui non potrebbero beneficiare svelando la loro vera identità. In questo modo si possono infiltrare in gruppi di contatti altrimenti inaccessibili o stringere amicizie su Internet con persone che le tratterebbero diversamente alla luce della loro vera identità.

Identità rubate o inventate possono essere utilizzate a diversi fini malevoli, come per esempio per raccogliere informazioni per scopi illegali e per l'adescamento di minori su Internet, atti persecutori su Internet, bullismo su Internet, *phishing* (furto elettronico di dati), *spamming* (invio di messaggi pubblicitari indesiderati tramite la posta elettronica) o anche per la diffusione di virus su computer.

4.4.3.2 Soluzioni adottate all'estero o nel diritto internazionale

La raccomandazione del Consiglio d'Europa relativa alle reti sociali sollecita la creazione di meccanismi di ricorso adeguati contro il comportamento malintenzionato nelle reti sociali, concentrandosi particolarmente sul furto d'identità. Gli Stati membri dovrebbero obbligare i gestori delle piattaforme ad adottare le misure di sicurezza più efficaci per proteggere i dati personali dall'accesso illegale di terzi. Il che dovrà comprendere anche il criptaggio della comunicazione tra utente e il sito web del gestore della piattaforma. Inoltre i gestori delle piattaforme dovrebbero informare gli utenti in merito a violazioni delle misure di sicurezza affinché questi possano adottare delle misure di prevenzione, come per esempio il cambiamento della propria parola chiave.

La Commissione europea propone l'istituzione di un Centro europeo per la lotta alla criminalità informatica[143], che tra le altre cose dovrà dedicarsi alla protezione dei profili utenti nelle reti sociali contro l'abuso digitale per poter procedere contro il furto d'identità su Internet[144].

4.4.3.3 Situazione legale in Svizzera

Se nelle reti sociali soggetti terzi creano profili utenti avvalendosi di un nome protetto giuridicamente e senza il consenso dell'avente diritto, violano normalmente la protezione del nome proprio sul piano del diritto civile ai sensi dell'articolo 29 capoverso 2 CC. La prescrizione tutela la persona interessata dall'indebita usurpazione del proprio nome da parte di terzi. Questa comprende nomi civili e ufficiali di persone fisiche, ma anche pseudonimi, nomignoli, sigle abbreviate, acronimi e nomi abbreviati, purché nella comunicazione essi siano intesi come il nome di un soggetto denominato[145].

Vi è violazione del diritto alla propria immagine di cui all'articolo 28 CC, se persone non autorizzate utilizzano immagini di un'altra persona per creare un profilo utente avvalendosi della sua identità.

Nelle reti sociali che servono anche alla comunicazione privata (per esempio Facebook), è considerata una violazione della sfera personale riservata di cui all'artico 28 CC il fatto che un terzo si infiltri in profili utente altrui e in questo modo venga a conoscenza della comunicazione privata a cui la persona in questione non gli ha dato accesso. Il divieto riguarda anche l'utilizzo di profili utente altrui o creati in nome di estranei per indurre terzi, tramite un'identità simulata, a svelare informazioni private.

---

[143] Comunicazione «Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica», COM(2012) 140 definitivo.

[144] Comunicato stampa della Commissione europea del 28.03.2012 «Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica», IP/12/317.

[145] *BSK-ZGB I*, Bühler Roland, 4ª ed., Basilea 2010, art. 29, pag. 321 seg. n. marg. 4, 7, pag. 325 n. marg. 16.

Sul piano del diritto della protezione dei dati, raccogliere dati personali fornendo una falsa identità costituisce una violazione del principio della riconoscibilità della raccolta dei dati e del principio della buona fede (art. 4 cpv. 2 e 4 LPD) [146]. Se terzi pubblicano dati personali degni di particolare protezione della persona interessata in un profilo utente creato avvalendosi di un nome altrui, infrangono l'articolo 12 capoverso 2 lettera c LPD.

Se terzi si infiltrano abusivamente tramite atti di pirateria informatica in profili utenti altrui e qui attingono a informazioni che non sono accessibili pubblicamente, vi modificano contenuti o parole chiave d'accesso degli aventi diritto, potrebbero valere le fattispecie penali dell'accesso indebito a un sistema per l'elaborazione di dati (art. 143bis CP), del danneggiamento di dati (art. 144bis CP) e della sottrazione indebita di dati personali (art. 179^{novies} CP).

Profili utente creati avvalendosi di un'identità altrui e profili con un'identità immaginaria possono servire ai fini illeciti più svariati. In primo piano vi sono i reati contro il patrimonio e i delitti contro l'onore, come anche la coazione o le minacce (art. 173-177, 146, 147, 156, 180, 181 PC), nonché le lesioni della personalità e gli atti persecutori su Internet (art. 28, 28*b* cpv. 1 n. 3 CC). L'articolo 3 capoverso 1 lettera o LCSl tutela contro lo *spamming*, mentre l'articolo 144bis numero 1 CP contempla il danneggiamento di dati nonché l'impiego e la diffusione di virus (anche) tramite reti sociali digitali.

Contro *phishing* e la diffusione di *malware* sui domini .ch si può procedere in modo efficace ai sensi dell'articolo 14bis dell'ordinanza del 6 ottobre 1997 concernente gli elementi d'indirizzo nel settore delle telecomunicazioni (ORAT)[147]. Nei singoli casi la sua applicazione può essere utile anche per perseguire legalmente l'impiego di un'identità altrui.

Dall'analisi risulta che il diritto materiale contempla ampiamente azioni legate all'uso abusivo di un'identità altrui tramite mezzi digitali. In realtà, soprattutto nel caso di delinquenti professionisti, è difficile risalire all'identità per poter procedere contro di loro.

4.4.4 Osservazione di affermazioni sui media sociali digitali (*social media monitoring* – monitoraggio dei media sociali digitali)

4.4.4.1 Situazione iniziale

Imprese, autorità, organizzazioni e determinati privati sono interessati a sapere cosa venga riportato sul loro conto nei media sociali digitali. Tramite un'osservazione sistematica e costante, le organizzazioni interessate cercano di ottenere (o riottenere) il controllo sulla propria immagine. Per gestire il flusso d'informazioni caotico si ricorre a strumenti automatizzati.

Il problema del monitoraggio dei media sociali digitali è che non vengono coinvolti solo i contenuti di informazioni diffuse nella rete sociale ma anche le indicazioni riguardanti i relativi autori. Chi osserva ottiene informazioni in merito al vero nome o almeno allo pseudonimo dell'autore, tra cui anche l'età, il sesso, la professione, il datore di lavoro, il luogo d'origine ed eventualmente anche ad altri dati resi pubblici. Particolarmente delicate sono per esempio le informazioni in merito alla visione del mondo e alle idee politiche.

4.4.4.2 Situazione legale in Svizzera

Non tutti i trattamenti dei dati possibili sul piano tecnico nelle reti sociali fanno necessariamente capo al principio dell'uso vincolato dei dati. Anche i dati pubblicati non possono essere semplicemente utilizzati per altre finalità secondo la legge sulla protezione dei dati. I dati personali presenti su piattaforme di media sociali digitali sono spesso indirizzati soltanto a persone amiche o vengono resi pubblici solo in una determinata situazione o contesto. Senza informazioni trasparenti relative al monitoraggio dei media sociali digitali, alle persone interessate mancano per lo meno le conoscenze necessarie in

---

[146] Rosenthal David/Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 81 n. 14, pag. 99 n. 56.

[147] RS **784.104**

merito all'impiego dei dati personali per il monitoraggio. I membri delle piattaforme dei media sociali digitali devono almeno poter riconoscere dalle circostanze che sono impiegati strumenti di monitoraggio. Se sono pubblicati dati personali relativi a terzi,ciò è avvenuto comunque senza che questi abbiano espresso la propria volontà e ne fossero a conoscenza. Per tali motivi in molti casi non si può presupporre che le persone interessate abbiano reso pubblicamente accessibili i propri dati personali sulle piattaforme dei media sociali digitali ai sensi dell'articolo 12 capoverso 3 LPD.

Sul suo sito Internet l'IFPDT ha rilasciato raccomandazioni per un impiego del monitoraggio dei media sociali conforme alla protezione dei dati[148]. Il trattamento di dati personali dovrà tuttavia limitarsi essenzialmente ai fini dell'analisi e tali dati dovranno essere cancellati o resi anonimi il più presto possibile. I dati personali non pubblici (in particolare quelli provenienti da gruppi chiusi di utenti o da cerchie di amici) dovrebbero essere esclusi. Il monitoraggio dovrebbe limitarsi a un'analisi di opinioni e di commenti pubblici.

4.5 Pregiudizio dell'interesse generale

4.5.1 Affermazioni razziste e altre esternazioni discriminanti (hate speech)

4.5.1.1 Situazione iniziale

Internet in generale, e le reti sociali in particolare, offrono una piattaforma ideale per diffondere esternazioni razziste tramite immagini, testi e video[149] e rappresentano un ottimo strumento perorganizzare associazioni razziste e reclutare nuovi membri.

Le reti sociali possono anche essere utilizzate per discriminare persone in base a criteri diversi dalla razza, come ad esempio l'orientamento sessuale, l'origine, la religione, le menomazioni fisiche, mentali o psichiche, il modo di vita, la lingua, la posizione sociale, le convinzioni politiche o le visioni del mondo, il sesso o l'età.

Rispetto alle pagine web, nelle reti sociali è ancora più difficile controllare e rimuovere contenuti razzisti e discriminanti. Infatti, in questi forum la diffusione di contenuti e il collegamento in rete delle persone avviene in modo ancora più semplice e rapido.

Le procedure contro esternazioni discriminanti nelle reti sociali possono urtarsi ai diversi quadri legali che i vari Stati prevedono per i contenuti razzisti o in altro modo discriminanti, alcuni possono ad esempio essere legali all'estero e punibili in Svizzera[150]. Nei media internazionalmente accessibili ciò crea difficoltà, si osserva la tendenza generale dei gestori a bloccare pagine e contenuti su richiesta dei Paesi in cui tali contenuti sono punibili. Si pensi a Twitter, che ha bloccato il conto utente di un'associazione di estrema destra vietata in Germania, per i suoi utenti che nel proprio profilo hanno indicato la Germania come loro Paese d'origine[151].

4.5.1.2 Soluzioni adottate all'estero o nel diritto internazionale

Il protocollo aggiuntivo alla Convenzione del Consiglio d'Europa sulla cibercriminalità concernente gli atti di natura razzista o xenofoba commessi attraverso i sistemi informatici del 28 gennaio 2003 è orientato esplicitamente alla diffusione in Internet di contenuti razzisti e xenofobi. Il 1° gennaio 2012, la

---

[148] http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00692/

[149] Secondo una comunicazione interna dello SCOCI relativa al suo rapporto annuale 2011, nove sulla trentina di discriminazioni razziali segnalate nel 2011 sono state perpetrate tramite le reti sociali.

[150] Negli Stati Uniti ad es. "hate speech" gode di una protezione molto maggiore rispetto alla maggior parte dei Paesi dell'Europa occidentale. Si pensi alla sentenza del Tribunal de Grande Instance de Paris "LICRA v. Yahoo!" del 22.05.2000, nella quale il tribunale francese ha dichiarato illegale la vendita di memorabilie naziste sul sito delle aste online Yahoo – cosa che è invece autorizzata secondo il diritto U.S.

[151] Cfr. articolo "Erste landesspezifische Sperre auf Twitter: Account von verbotener rechtsextremistischer Vereinigung in Deutschland gesperrt"; consultabile all'indirizzo: https://netzpolitik.org/2012/erste-landesspezifische-sperre-auf-twitter-account-von-verbotener-rechtsextremistischer-vereinigung-in-deutschland-gesperrt/ .

Svizzera ha sottoscritto la Convenzione del Consiglio d'Europa del 24 novembre 2001 sulla cibercriminalità[152]. Pur essendo stato approvato dal Consiglio federale, il protocollo aggiuntivo non è ancora entrato in vigore per la Svizzera.

In base al § 18 del trattato sulla tutela dei giovani dai rischi dei media (Jugendmedienschutz-Staatsvertrag)[153] tra i Länder tedeschi, è stato creato il servizio «jugendschutz.net»[154] che in Germania procede molto attivamente contro i contenuti razzisti o discriminanti in Internet e nelle reti sociali. L'organizzazione sensibilizza inoltre l'opinione pubblica mediante giornate sulla prevenzione, corsi di perfezionamento o pubblicazioni, come ad esempio «Klickt's? Geh Nazis nicht ins Netz!»[155] Il suo lavoro mira a contrastare l'ampio utilizzo delle reti sociali da parte degli ambienti di estrema destra. Un'altra piattaforma tedesca dall'orientamento analogo è Netz-Gegen-Nazis.de[156].

La fondazione INACH (International Network Against Cyberhate)[157], creata da jugendschutz.net interviene in modo transnazionale contro la diffusione e l'istigazione all'odio in Internet, e in particolare contro il mobbing nelle reti sociali. È una rete internazionale con rappresentanze in vari Stati che si scambiano strategie di buona prassi e si adoperano per rimuovere da Internet contenuti e siti web discriminanti e punibili.

4.5.1.3 Situazione legale in Svizzera

L'articolo 261bis del Codice penale vieta diverse forme di discriminazione contro una persona o un gruppo di persone per la loro razza, etnia o religione da parte di privati. La disposizione comprende in linea di massima tutte le forme di comunicazione possibili nelle reti sociali, ovvero foto, video, immagini o testi. A condizione, però, che si tratti di comunicazione *pubblica*[158]. La dottrina giuridica[159] considera pubbliche le esternazioni sulle reti sociali, che non si rivolgono soltanto a singole persone legate da un rapporto di fiducia (ad es. tramite impostazioni restrittive della sfera privata su Facebook).

Nella prassi giudiziaria svizzera si è già assistito a diverse condanne dovute a affermazioni razziste nelle reti sociali.[160] L'articolo 261bis CP contempla solo le discriminazioni in base a razza, etnia o religione e quindi non tutte le caratteristiche elencate nel divieto di discriminazione sancito dalla Costituzione (Art. 8 cpv. 2 Cost.) quali sesso, età, menomazioni fisiche, mentali o psichiche o orientamento sessuale. Il diritto della personalità (art. 28 seg. Cost.) è l'unico a garantire una certa protezione qualora, nelle reti sociali, una persona venga discriminata in base ad altri criteri.

A livello federale la Commissione federale contro il razzismo (CFR)[161] e il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet (SCOCI)[162] si occupano di procedere contro il razzismo in Internet. Se la CFR nota esternazioni razziste su determinate reti sociali, lo comunica allo SCOCI che, dopo aver effettuato un primo esame e memorizzato i dati, inoltra le segnalazioni [163] alle

---

[152] RS **0.311.43**.

[153] Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien dal 10 al 27.09.2002, Bay.GVBI N. 5/2003, pag. 147 segg.

[154] http://www.jugendschutz.net/.

[155] http://www.jugendschutz.net/materialien/klickts.html.

[156] http://www.netz-gegen-nazis.de/.

[157] http://www.inach.net/index.php .

[158] Per un'interpretazione in senso lato del termine *pubblico* da parte del Tribunale federale si veda la DTF **130** IV 111.

[159] Cfr. Fiolka Gerhard, Basler Kommentar Strafrecht II, terza ed. Basilea 2013, passo antecedente l'art. 258 n. 25.

[160] Si pensi al commento su Facebook rivolto a un'allieva di colore (decisione n. 2010-32 nella raccolta di casi giuridici della Commissione federale contro il razzismo; http://www.ekr.admin.ch/dienstleistungen/00169/index.html?lang=it)

[161] http://www.ekr.admin.ch/aktuell/index.html?lang=it.

[162] http://www.cybercrime.admin.ch/content/kobik/it.

[163] °Nel 2012 la quota di segnalazioni dovute a discriminazione razziale ammontava solo allo 0,78 per cento di tutte le segnalazioni; rapporto annuale SCOCI 2012, pag. 4.

autorità preposte al perseguimento penale nazionali o estere. Lo SCOCI agisce anche su iniziativa personale: perquisisce Internet alla ricerca di contenuti rilevanti dal punto di vista penale ed effettua analisi approfondite sulla criminalità in Internet. Dato che i gestori di molte reti sociali hanno sede all'estero, la persecuzione penale risulta spesso difficile, soprattutto quando si tratta di scoprire la vera identità di un autore. Stando allo SCOCI, nella prassi la rimozione di contenuti potenzialmente punibili non risulta essere un problema di fondo. Le condizioni d'utilizzo di molte reti sociali vietano la diffusione di contenuti a carattere razzista o oltremodo discriminanti, se ne viene segnalata la presenza, in linea di massima i gestori procedono alla loro cancellazione.

4.5.2 Pornografia

4.5.2.1 Situazione iniziale

La diffusione di pornografia tramite le reti sociali crea problemi analoghi a quella su Internet in generale, se rientra nella categoria della pornografia dura (ossia conformemente all'art 197 n. 3 CP ad es. la rappresentazione di atti sessuali con bambini o animali) o se si tratta di pornografia leggera accessibile a persone sotto i 16 anni. Nel presente rapporto ci soffermiamo in particolare sulla pedopornografia.

I contenuti a carattere pedopornografico sono vietati a livello mondiale, chi intende diffonderli via Internet utilizza generalmente canali più anonimi e segreti rispetto alle classiche reti sociali. Rappresentazioni di violenza sessuale nei confronti di bambini vengono vendute su siti web commerciali o scambiate in gruppi chiusi o tramite reti peer-to-peer[164]. Quest'ultima soluzione permette uno scambio discreto e anonimo del materiale pedopornografico[165]. Nella prassi, la pubblicazione o la diffusione di contenuti a carattere pedopornografico su piattaforme aperte è piuttosto rara.

4.5.2.2 Soluzioni adottate all'estero o nel diritto internazionale

La Convenzione sulla cibercriminalità del 23 novembre 2001 (RS *0.311.43*) è vincolante anche per la Svizzera e mira all'avvicinamento delle legislazioni a livello internazionale e a migliorare la collaborazione tra gli Stati contraenti, un fatto importante questo, poiché le questioni inerenti Internet spesso esulano dai confini nazionali. L'articolo 9 della Convenzione contiene disposizioni relativamente complete sulla punibilità di atti in relazione alla pedopornografia.

Diverse organizzazioni in vari Stati si dedicano alla ricerca e alla rimozione di contenuti dannosi e illegali in Internet. In Inghilterra è attiva ad esempio la Internet Watch Foundation che si occupa tra l'altro di rintracciare contenuti a carattere pedopornografico[166].

Presumibilmente, a seguito dell'adesione della Svizzera alla Convenzione del Consiglio d'Europa del 25.10.2007 per la protezione dei minori contro lo sfruttamento e gli abusi sessuali, in futuro saranno punibili anche il consumo intenzionale di pornografia dura, il che comprende anche la sola visualizzazione di quest'ultima nelle reti sociali, senza scaricamento dei contenuti[167].

4.5.2.3 Situazione legale in Svizzera

L'articolo 197 CP tutela le persone minori di 16 anni da qualsiasi tipo di confronto con la pornografia e gli adulti da quella non richiesta, vietando la pornografia dura. Elenca la maggior parte delle azioni o degli oggetti del reato in grado di inoltrare, tramite le reti sociali, pornografia leggera ai falsi destinatari, o diffondere o rendere reperibile pornografia dura. Se sulle reti sociali, ad esempio in forma di un video Youtube, vegnono diffusi contenuti pornografici senza un'efficace restrizione d'accesso, questi

---

[164] Informazione del Servizio di coordinazione per la lotta contro la criminalità su Internet in merito alla pedopornografia, http://www.cybercrime.admin.ch/content/kobik/it/home/themen/kinderpornografie.html.

[165] Cfr. comunicati stampa dell'Ufficio federale di polizia "Calano le comunicazioni di sospetto: la pedopornografia resta tuttavia la categoria con il maggior numero di segnalazioni inviate a SCOCI" del 03.04.2012, http://www.fedpol.admin.ch/content/fedpol/it/home/dokumentation/medieninformationen/2012/2012-04-03.html.

[166] http://www.iwf.org.uk/ .

[167] FF **2012** 6805 e FF **2012** 6841.

diventano accessibili a persone minori di 16 anni. Un segnale d'avvertimento su un sito Internet, che sparisce dopo averci cliccato sopra, non basta[168], e neppure una limitazione d'uso di un sito web tramite password se non viene verificata l'età[169].

I contenuti pornografici, compresa la pornografia leggera, rientrano in quella categoria di contenuti normalmente vietati nelle condizioni d'utilizzo della maggior parte dei gestori di piattaforme. Se dovessero comunque apparire possono essere rimossi in modo abbastanza rapido e semplice grazie a funzioni di «Notice-and-Take-down» e programmi di filtraggio piuttosto rigidi. I canali, spesso internazionali, attraverso i quali viene diffusa la pornografia illegale mettono a dura prova le autorità di perseguimento penale, soprattutto per via delle differenze nei vari ordinamenti giuridici in quanto a prescrizioni e misure. Il numero di segnalazioni inoltrate allo SCOCI a causa di pornografia vietata (soprattutto pedopornografia) è costantemente elevato. A livello federale, inoltre, lo SCOCI indaga anche sulla pedopornografia e avvia ricerche indipendentemente dalla presenza di un sospetto.[170]

4.5.3 Minaccia dell'ordine pubblico attraverso la mobilitazione di massa

4.5.3.1 Situazione iniziale

Le piattaforme sociali hanno un potenziale prezioso per la società democratica, permettono infatti, soprattutto alle minoranze, di formarsi un'opinione e di avere voce in capitolo. In una data costellazione sono in grado di mobilizzare entro breve tempo una grande massa di persone.[171] In casi estremi ciò può avere anche effetti negativi e compromettere l'ordine pubblico.

Si pensi all'appello lanciato su Facebook a partecipare a una manifestazione di massa dal tema «Tanz dich frei», in occasione della quale una minoranza di persone predisposte all'uso della violenza ha creato, nel maggio 2013, ingenti danni nel nucleo di Berna. In quanto attore privato nella procedura penale, la città ha chiesto tra l'altro di ordinare all'impresa Facebook di fornire i dati relativi al conto utente dal quale è stato lanciato l'appello. [172]

4.5.3.2 Soluzioni adottate all'estero o nel diritto internazionale

I problemi della mobilitazione attraverso le reti sociali possono essere illustrati sull'esempio dei violenti scontri avvenuti il 21 settembre 2012 nella cittadina neerlandese di Haren. A suscitare scompiglio è stato un post di una giovane su Facebook che aveva dimenticato di specificare che l'invito alla festa dei suoi 16 anni era privato. Su Twitter e Facebook è quindi stato pubblicato un appello, diffusosi a macchi d'olio, a recarsi alla festa «Projekt-X-Fest» al quale hanno fatto seguito migliaia di giovani. L'atmosfera inizialmente pacifica è degenerata, non da ultimo a causa dell'alcool, in una situazione molto aggressiva alla quale, per motivi vari, le forze dell'ordine non hanno potuto far fronte.

In un rapporto pubblicato nel marzo 2013 una commissione d'inchiesta ha proposto tra l'altro che le autorità vengano istruite sul funzionamento dei media sociali. Grazie a un accurato monitoraggio delle piattaforme dovrebbero in futuro essere in grado di riconoscere e sventare a tempo tali pericoli per l'ordine pubblico, senza tuttavia sorvegliare sistematicamente le singole persone, e chiedere immediatamente ai gestori di piattaforme sociali di rimuovere questi appelli ad attività illecite. Inoltre, gli opera-

---

[168] DTF **131** IV 64 consid. 10.3

[169] Sentenza del Tribunale federale 6S.26/2005 consid. 3.2

[170] °Nel 2012, le segnalazioni di sospetto a causa di pedopornografia vietata rappresentavano circa un terzo di tutte le segnalazioni; rapporto annuale SCOCI 2012, pag. 4.

[171] In merito alle opportunità offerte dai media sociali per una comunicazione variegata e viva, cfr. punto 3.2.

[172] °Comunicato stampa della città di Berna del 12 giugno 2013: http://www.bern.ch/mediencenter/aktuell_ptk_sta/2013/06/strafanzeige/view?searchterm=tanz dich frei

tori dovrebbero informare soprattutto la loro giovane clientela sui rischi che nasconde la mescolanza di comunicazioni private e pubbliche sui media sociali.[173]

4.5.3.3 Situazione legale in Svizzera

Chiunque intenzionalmente determina altri a commettere un atto illecito concreto (ad es. danno materiale), rischia una pena per istigazione a tale delitto (art. 24 CP). In questo caso l'istigatore rischia la stessa pena applicabile all'autore. Inoltre, il Codice penale svizzero punisce la pubblica istigazione a un crimine o a commettere un delitto implicante atti di violenza contro persone o cose, con una pena detentiva sino a tre anni o con una pena pecuniaria (art. 259 CP). L'appello non deve rivolgersi ad atti ben precisi né orientarsi a persone chiaramente definite. Secondo la prassi deve però presentare una certa enfasi, un'istigazione eloquente può però presentarsi anche se qualcuno fa suoi i messaggi di altri (retweet)[174].

Non è punibile invece, il semplice appello a partecipare a una manifestazione non autorizzata. Quest'ultimo può per contro ledere prescrizioni cantonali o comunali[175].

Analogamente ad altre disposizioni penali (ad es. norma penale contro la discriminazione razziale, cfr. punto 4.5.1.3) all'articolo 259 CP sulle piattaforme sociali, si pone il problema di sapere se un'esternazione va considerata privata o pubblica.

Come per le lesioni dell'onore, anche l'istigazione secondo l'articolo 259 può rientrare nella regolamentazione speciale sulla punibilità dei media (art. 28 CP)[176]. Secondo questa prescrizione è punibile solo l'autore dell'istigazione pubblica, e soltanto in sua vece – qualora l'autore non possa essere individuato o non possa essere tradotto davanti a un tribunale svizzero – il redattore responsabile o la persona responsabile della pubblicazione).

In merito alla persecuzione degli autori di contenuti illeciti su piattaforme online, si veda il punto 5.2 e in merito alle misure di blocco e di cancellazione il punto 5.4

4.5.4 Minaccia della salute pubblica

4.5.4.1 Situazione iniziale

Le reti sociali vengono utilizzate per scambiarsi opinioni sugli interessi più svariati. A seconda dell'argomento e della motivazione ciò può avere anche effetti dannosi sulla società o sulla salute degli utenti. Infatti, i forum online in cui gli interessati si scambiano opinioni sul suicidio, sull'anoressia o sull'autolesionismo, possono idealizzare o addirittura stimolare o favorire questo tipo di comportamento e di fenomeni. Ciò può portare a una banalizzazione del problema, rafforzare tendenze all'autolesionismo già presenti e nella peggiore delle ipotesi portare alla messa in pratica di questi comportamenti dannosi. Oltre ai rischi, Internet offre però anche informazioni utili per affrontare tali problemi[177].

Un altro problema è costituito dai numerosi forum presenti in Internet che permettono lo scambio di informazioni su malattie, medicinali e metodi terapeutici, la cui qualità non è o è difficilmente verificabile. Il 44 per cento della popolazione svizzera attinge in Internet informazioni relative alla salute, spesso a complemento delle informazioni avute da esperti o da persone di fiducia. Si presuppone che aumenterà la domanda di trovare in Internet informazioni sulla salute e applicazioni Internet partecipative. Due persone su tre, che si informano su questioni inerenti la salute, non si fidano completamente

---

[173] Rapporto della commissione "Project X – Haren" del 8.3.2013, pag. 31 segg.; scaricabile in neerlandese all'indirizzo: http://de.scribd.com/doc/129273298/Hoofdrapport-rellen-Haren

[174] Fiolka Gerhard, Basler Kommentar Strafrecht II, terza ed. Basilea 2013, art. 259 n. 12

[175] Cfr. art. 8 del regolamento della città di Berna concernente i comizi su suolo pubblico http://www.bern.ch/leben_in_bern/stadt/recht/dateien/143.1/

[176] Cfr. Zeller Franz, *Basler Kommentar Strafrecht* II, terza ed. Basilea 2013, art. 28 n.65.

[177] Cfr. Gruppo di lavoro sulle disfunzioni alimentari (AES): www.aes.ch (sito in tedesco).

delle informazioni trovate in rete[178]. Questa fetta di popolazione si sente rassicurata dall'allestimento di controlli o certificati nel settore online della sanità. Per gli utenti meno diffidenti rimane il rischio che sui portali online trovino risposte inerenti la salute poco professionali o addirittura errate, il che, nel peggiore dei casi, può portare a conseguenze negative per la salute.

4.5.4.2 Soluzioni adottate all'estero o nel diritto internazionale

Il servizio «jugendschutz.net» fondato dai Länder tedeschi informa anche sui pericoli e sui rischi in relazione a portali pericolosi per i giovani, che glorificano o promuovono il suicidio, l'anoressia e l'autolesionismo[179]. «jugendschutz.net» informa i diretti interessati ei genitori, verifica siti Internet pertinenti e si adopera per rimuovere contenuti problematici. Inoltre, sensibilizza i gestori delle reti sociali riguardo al tema e offre a coloro che desiderano rimuovere tali contenuti un sito web di sostituzione sul tema inerente i disturbi del comportamento alimentare che rinvia a campagne di sensibilizzazione e servizi di consulenza[180].

Conformemente al § 18 cpv. 1 della legge tedesca sulla tutela dei giovani (deutsches Jugendschutzgesetz[181]), l'organo di sorveglianza competente[182] può collocare su una lista nera supporti e mezzi di telecomunicazione suscettibili di pregiudicare lo sviluppo di bambini o giovani. L'indicizzazione dell'organo di sorveglianza comprende tra l'altro forum che glorificano l'anoressia o il suicidio[183].

4.5.4.3 Situazione legale in Svizzera

Lo scambio tra privati aventi gli stessi interessi relativi a suicidio, anoressia, autolesionismo, ecc. rientra in generale nel campo della libertà d'opinione. Non vi sono basi legali che trattano concretamente il fenomeno qualora dovesse risultare di avere ripercussioni negative sulla società. In linea di massima la Confederazione può intervenire a titolo informativo per tutelare la salute della popolazione. L'Ufficio federale della sanità pubblica (UFSP) è attivo su vari fronti che presentano interfacce con argomenti relativi a suicidio, anoressia e autolesionismo. Finora l'UFSP non si è però occupato esplicitamente di azioni dannose per la salute eventualmente veicolate dai social media.

Attualmente non vi è alcuna base legale che limiti lo scambio di opinioni tra privati su medicamenti o metodi terapeutici, a condizione che essi non intraprendano attività pubblicitarie[184]. L'UFSP auspica maggiore trasparenza per quanto riguarda le informazioni sulla salute e i forum sulla salute presenti in Internet. Gli attuali marchi di qualità attribuiti in Internet alle informazioni serie sulla salute[185] si riferiscono innanzitutto ai siti web e meno ai media sociali.

4.5.5 Manipolazione dell'opinione a fini commerciali

4.5.5.1 Situazione iniziale

Vi sono imprese che abusano delle reti sociali per diffondere informazioni positive o fuorvianti su prodotti o servizi, a tale scopo pagano degli attori che assumono il ruolo di consumatori indipendenti. Pur essendo in pochi, riescono a simulare attività di un gruppo ben più numeroso. A tale scopo possono

---

[178] Cfr. Rapporto eHealth Suisse, portale pubblico sulla salute, adottato dal comitato direttivo il 26.01.2012, pag. 6,7,11.

[179] http://www.jugendschutz.net/selbstgefaehrdung/index.html .

[180] http://www.anaundmia.de/ .

[181] Jugendschutzgesetz (JuSchG) (Legge sulla tutela dei giovani) del 23.07.2002, BGBl. I pag. 2730.

[182] http://www.bundespruefstelle.de/ .

[183] Cfr. decisione della Bundesprüfstelle zur Indexierung eines Magersucht-Blogs: Sentenza del BPjM n. 5601 del 04.12.2008 – "Pro Ana": http://www.doerre.com/jugendschutz/20081204_bpjm_index.pdf .

[184] Articolo 31 seg. legge federale del 15.12.2000 sui medicamenti e i dispositivi medici (LATer), RS **812.212.5** e l'ordinanza del 17.10.2001 sulla pubblicità dei medicamenti (OPuM), RS 812.212.5 che all'articolo 4 lett. c stabilisce che per pubblicità professionale s'intende la pubblicità di medicamenti mediante l'impiego di mezzi audiovisivi e di altri supporti video, audio, di dati e mediante altri sistemi di trasmissione di dati, per esempio Internet.

[185] Si pensi ai marchi di qualità della fondazione Health on the Net HON, www.hon.ch

anche avvalersi di falsi blog, i cosiddetti flog (fake blog) o sockpuppet (false identità online), che sembrano provenire da persone indipendenti ma sono invece allestiti solo a fini pubblicitari. Questi metodi possono essere impiegati anche per mettere in cattiva luce imprese concorrenti e discreditare le loro offerte.

Altri problemi possono sorgere anche dal formato di comunicazione di una piattaforma sociale. Si pensi a Twitter, i cui testi sono limitati a 140 segni e se viene utilizzato a scopi pubblicitari, non offre abbastanza spazio per citare le fonti, i motivi e le cause.

4.5.5.2 Soluzioni adottate all'estero o nel diritto internazionale

Anche in seno all'UE si comincia a reagire al fenomeno dei metodi di pubblicità non trasparenti nelle reti sociali[186]. La direttiva UE sui diritti dei consumatori[187], che disciplina la stipula di contratti tra aziende e consumatori, si occupa dell'adempimento degli obblighi d'informazione delle imprese considerando i vincoli tecnici, come ad esempio il numero limitato di segni su schermi piccoli. La direttiva formula requisiti minimi concernenti l'obbligo di informazione e chiede che i consumatori vengano rinviati ad altre fonti d'informazione, si pensi ai numeri gratuiti o ai link ipertestuali verso il sito web dell'impresa. In relazione alle reti sociali, questa regolamentazione è interessante nella misura in cui determinate offerte, come ed esempio Twitter, si caratterizzano da un numero limitato di segni. Inoltre, sempre più utenti accedono alle reti sociali attraverso mezzi di comunicazione mobile, si crea quindi un problema di informazione e di spazio dovuto ai limiti degli apparecchi terminali (ad es. smartphone).

L'ente statunitense per la protezione dei consumatori e per il diritto in materia di concorrenza (Federal Trade Commission; FTC) ha emanato direttive tese alla protezione dei consumatori da pubblicità sleale o ingannevole[188], che dovrebbero aiutare chi fa pubblicità a rispettare il diritto vigente[189]. Le direttive chiedono che nelle attività pubblicitarie sulle reti sociali (comprese quelle che offrono un numero limitato di caratteri come ad es. Twitter) vengano segnalati i legami finanziari e materiali (pagamenti o regali) tra le parti concorrenti e i terzi che effettuano pubblicità a loro nome (soprattutto blogger, persone celebri, ecc.)[190].

4.5.5.3 Situazione legale in Svizzera

Le disposizioni della legge federale contro la concorrenza sleale[191], che disciplinano l'attività pubblicitaria indipendentemente dai prodotti, settori o media, si applicano anche a Internet e quindi anche alle attività pubblicitarie sulle reti sociali[192].

---

[186] Nella decisione sull'influenza della pubblicità sul comportamento dei consumatori (2010/2052(INI)) (n. 17) il Parlamento europeo critica le nuove forme di pubblicità occulta in Internet, che non rientrano nella diriettiva sulle pratiche commerciali sleali. Si riferisce in questo caso ai commenti commerciali e alle notizie pubblicitarie di aziende in blog, reti sociali o forum simili che danno l'impressione di essere opinioni di consumatori indipendenti. Il Parlamento invita gli Stati membri a introdurre degli osservatori per verificare la presenza di pubblicità occulta in tali forum.

[187] Direttiva 2011/83/UE sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE e che abroga la direttiva 85/577/CEE e la direttiva 97/7/CE.

[188] Guides Concerning the Use of Endorsements and Testimonials in Advertising, FTC 16 CFR Part 255; consultabile all'indirizzo: http://www.ftc.gov/os/2009/10/091005revisedendorsementguides.pdf .

[189] In particolare Section 5 Federal Trade Commission Act (15 U.S.C. 45) to the use of endorsements and testimonials in advertising; consultabile all'indirizzo: http://www.ftc.gov/ogc/ftcact.shtm. La FTC sorveglia il rispetto delle direttive, in caso di violazione l'ente può procedere a un'indagine per stabilire se la prassi in questione viola il diritto in vigore, si veda in tal senso: http://www.ftc.gov/opa/2009/10/endortest.shtm .

[190] Le direttive consigliano inoltre alle parti attive nella pubblicità di informare esaustivamente i blogger, le persone celebri e chiunque faccia pubblicità per loro, sulle caratteristiche del prodotto e sulla situazione legale onde evitare dichiarazioni pubblicitarie fuorvianti. Inoltre, sono tenuti a verificare l'esattezza e l'adeguatezza delle affermazioni pubblicitarie rilasciate dai terzi da loro assunti. Rispondono delle dichiarazioni errate e fuorvianti su un prodotto sia la parte attiva nella pubblicitarà, sia i terzi da essa assunti.

[191] Legge federale del 19.12.1986 contro la concorrenza sleale (LCSl), RS **241**.

[192] Jöhri Yvonne, *Werbung im Internet*, Zurigo 2000, pag. 59.

La clausola generale all'articolo 2 LCSl definisce sleale la pubblicità occulta ossia l'inganno sulla natura pubblicitaria degli atti di concorrenza[193]. Se, per aver espresso, sul proprio blog o profilo in una rete sociale, un giudizio positivo su una determinata impresa e la sua offerta, un privato riceve gratuitamente prodotti o una retribuzione dall'impresa in questione e se questo fatto non viene comunicato in modo trasparente, tale comportamento può risultare sleale conformemente (al principio sancito) all'articolo 2 LCSl[194], a condizione che il comportamento possa essere oggettivamente considerato in grado di influenzare la funzionalità del relativo mercato. Inoltre, la concorrenza sleale può essere disciplinata anche dall'articolo 3 capoverso 1 lettera b e i LSCl. Con l'ultima revisione della LSCl è stato introdotto l'articolo 3 capoverso 1 lettera s[195] che prevede l'obbligo vincolante di fornire informazioni tese a migliorare la trasparenza nel commercio elettronico.

Se persone terze, pagate o altrimenti retribuite vengono sollecitate da una società a utilizzare la loro presenza nelle reti sociali per mettere in cattiva luce concorrenti dell'impresa, può essere applicato l'articolo 3 capoverso 1 lettera a LCSl, a condizione che la procedura denigri altri, le sue merci, le sue opere, le sue prestazioni, i suoi prezzi o le sue relazioni d'affari con affermazioni inesatte, fallaci o inutilmente lesive[196]. In questo campo la difficoltà dovrebbe consistere soprattutto nel riconoscere il carattere pubblicitario delle presenze di privati sulle reti sociali e nel fornire le prove del legame tra privati e una determinata impresa.

4.5.6 Manipolazione della formazione dell'opinione pubblica (politica)

4.5.6.1 Situazione iniziale

Metodi analoghi a quelli del settore commerciale possono essere impiegati anche nel campo della formazione dell'opinione pubblica per influenzare il discorso politico: un fenomeno problematico soprattutto alla vigilia di elezioni o votazioni. Profili sulle piattaforme sociali, gruppi in rete o blog vengono sfruttati per promuovere candidati o determinati argomenti in votazione facendosi passare per voci indipendenti. Il fenomeno viene chiamato «astroturfing».

Inoltre, sono in fase di sviluppo programmi di software che dovrebbero permettere a persone singole di gestire diversi conti utenti in blog, forum su Internet e reti sociali, onde creare artificialmente delle maggioranze d'opinioni[197].

4.5.6.2 Situazione legale in Svizzera

La libertà di elezione e votazione conformemente all'articolo 34 capoverso 2 Cost. tutela in modo limitato anche dall'influenza di attori privati sulla libera formazione della volontà. Soprattutto alla vigilia di una votazione o elezione lo Stato è tenuto a garantire determinate misure di protezione. Se poco prima di un voto alle urne, privati diffondono contenuti esplicitamente errati o fuorvianti, le Autorità devono eventualmente informare gli aventi diritto al voto sul comportamento di tali persone o chiarire determinati contenuti. È possibile procedere a una nuova votazione nei casi in cui risulta probabile che il comportamento di privati abbia influenzato massicciamente il risultato delle votazioni e le Autorità non abbiano adempiuto il loro dovere d'informazione.

Per quanto riguarda le campagne politiche nascoste promosse sui media sociali, lo Stato deve quindi intervenire solo se l'occultamento dei veri moventi della presenza sui social media può fuorviare gli aventi diritto al voto e se ciò è avvenuto poco prima del termine delle votazioni. I risultati delle votazioni vengono dichiarati nulli solo se appare verosimile che siano stati influenzati in modo decisivo da questo tipo di metodi opachi. In assenza di prove, e se tale comportamento non rientra nel lasso di

---

[193] Jung Peter/Spitz Philippe (ed.), *Bundesgesetz gegen den unlauteren Wettbewerb*, Berna 2010, pag. 180 seg.; Weber Rolf/Volz Stephanie, *Online Marketing und Wettbewerbsrecht*, Zurigo 2011, pag. 52.

[194] Weber Rolf/Volz Stephanie, *Online Marketing und Wettbewerbsrecht*, Zurigo 2011, pag. 71 seg.

[195] FF **2011** 4402

[196] Jung Peter/Spitz Philippe (ed.), *Bundesgesetz gegen den unlauteren Wettbewerb*, Berna 2010, pag. 226 segg.

[197] "Security-Firma entwirft Tools zur Meinungsmache mit Kunstfiguren", heise online del 20.02.2011: http://www.heise.de/newsticker/meldung/Security-Firma-entwirft-Tools-zur-Meinungsmache-mit-Kunstfiguren-1193436.html .

tempo immediatamente precedente elezioni o votazioni, sarà la discussione pubblica a rettificare queste affermazioni errate o fuorvianti (di privati)[198]

4.5.7 Pubblicità vietata per determinati prodotti o prestazioni

4.5.7.1 Situazione di partenza

Allo scopo di tutelare determinati interessi pubblici in Svizzera vi sono diversi divieti di pubblicità che possono essere violati anche tramite la comunicazione nelle reti sociali. Si tratta ad esempio della pubblicità per il tabacco a quella per determinati agenti terapeutici.

Precario è ad esempio il rispetto delle regole contenute nella legge federale del 21 giugno 1932 sulle bevande distillate (Legge sull'alcool; RS *680*). Il Servizio di coordinamento del commercio e della pubblicità[199], responsabile del rispetto della legge sull'alcool si trova sempre più spesso a dover esaminare pagine su Facebook. In questo caso vi è il problema che spesso i contributi che non riguardano un prodotto non provengono dall'amministratore della pagina, ma sono stati inseriti da altri utenti "amici" su sua richiesta.

4.5.7.2 Situazione legale in Svizzera

La pubblicità nei media sociali orientata alla Svizzera deve rispettare in particolare le restrizioni pubblicitarie sancite all'articolo 42b della legge sull'alcool. Questa legge contiene anche prescrizioni per la tutela dei giovani: l'articolo 42b capoverso 3 lettera e della legge sull'alcool vieta la pubblicità per le bevande distillate «in occasione di manifestazioni cui partecipano soprattutto fanciulli e adolescenti o che sono organizzate precipuamente per loro». Attualmente non è ancora stato chiarito se tali manifestazioni potrebbero avvenire anche nelle reti sociali.

Nella prassi, oltre ai mezzi a disposizione nel diritto penale amministrativo, la Regia federale degli alcool sottolinea l'importanza delle prescrizioni sulla pubblicità attraverso decisioni di diritto amministrativo. Nel caso di affermazioni nelle reti sociali, l'applicazione di queste ultime solleva diverse questioni: a chi viene attribuito il contributo su una piattaforma? Come è possibile vincolare giuridicamente un fornitore commerciale di un profilo in una rete sociale con sede all'estero?

4.6 Particolare necessità di protezione

4.6.1 Bambini e giovani

4.6.1.1 Situazione iniziale

I rischi, che le reti sociali rappresentano per bambini e giovani, sono di natura diversa e vanno al di là dei limiti sopra descritti che possono compromettere gli interessi privati di qualsiasi utente. Pongono un problema particolare i contenuti non adatti o dannosi per i giovani o l'approccio da parte di terzi, soprattutto se motivato da intenti di natura sessuale[200]. Non tutti i bambini e i giovani hanno le dovute capacità tecniche e la consapevolezza per proteggersi dai rischi in relazione ai contatti problematici o alla comunicazione dei propri dati personali[201]. Inoltre, genitori e insegnanti spesso non dispongono

---

[198] Cfr.: Müller Jörg Paul/Schefer Markus, Grundrechte in der Schweiz, quarta ed., Berna 2008, pag. 618 seg. e Häfelin Ulrich/Haller Walter/Keller Helen, Schweizerisches Bundesstaatsrecht, ottava ed., Zurigo 2012, pag. 443 seg. n. 1392 segg.

[199] Il servizio di coordinamento del commercio e della pubblicità controlla solo gli annunci pubblicitari, che presentano un nesso univoco con la Svizzera (ad es. lingua, moneta o diffusione del prodotto).

[200] Uno studio attuale conferma che i giovani in Svizzera sono spesso vittime di molestie sessuali attraverso i media elettronici. Il 9,5 % dei ragazzi e il 28 % delle ragazze ha affermato di esserne coinvolto. Un'importante sottocategoria degli abusi sessuali senza contatto corporeo è data dalla cosiddetta cibervittimizzazione. I dati riguardano i media elettronici in generale, non solo le reti sociali, ma anche la comunicazione via cellulare, posta elettronica. Cfr. Studio Optimus 2 "Sexuelle Übergriffe an Kindern und Jugendlichen in der Schweiz", febbraio 2012, pag. 9, 29 seg., 96 seg.

[201] Stando allo studio "EU Kids Online 2011" che si basa su un rilevamento dati in 25 Stati europei, circa il 64 % dei bambini e giovani tra gli 11 e i 16 anni sanno come bloccare messaggi indesiderati provenienti da terzi e il 56 % sono in grado di modificare le proprie impostazioni della sfera privata nelle reti sociali. Queste cifre rilevano un'ampia minoranza di bambini e giovani privi delle conoscenze necessarie per tutelarsi in Internet. Inoltre il 29 % dei giovani tra i 9 e i 12 anni e il 27 % di quelli tra i 13 i 16 anni hanno reso pubblico il loro profilo tramite le impostazioni e un quinto di essi vi indica informazioni quali indirizzo e numero telefonico. Cfr. "EU Kids Online Final Report", settembre 2011, pag. 17.

della necessaria esperienza e del sapere per informare correttamente bambini e giovani sui rischi che incorrono nelle reti sociali. Un altro problema possono essere le amicizie tra allievi e insegnanti createsi nelle reti sociali, infatti presentano il rischio di una vicinanza inappropriata. Tali contatti in rete aprono una finestra sulla vita privata degli allievi o degli insegnanti, e possono compromettere i rapporti quotidiani a scuola.

Un ostacolo tecnico nell'attuazione di un'effettiva protezione dei giovani nelle reti sociali è costituito tra l'altro dall'incapacità dei sistemi finora sviluppati di verificare l'età degli utenti. Infatti, questi non sono in grado di garantire che l'età indicata dall'utente corrisponda al vero[202].

4.6.1.2 Soluzioni adottate all'estero o nel diritto internazionale

La Raccomandazione del Consiglio d'Europa relativa alle reti sociali chiede una particolare tutela dei bambini e dei giovani nell'utilizzo delle reti sociali. A tale scopo i fornitori dovrebbero prevedere misure di tutela preventive, sistemi di allerta per contenuti problematici e procedere contro il bullismo su Internet e l'adescamento di minori su Internet.

Il Consiglio d'Europa esorta inoltre gli Stati membri a esaminare possibilità di rimozione o cancellazione dei contenuti collocati in Internet da bambini che potrebbero nuocere alla loro dignità, sicurezza o alla loro sfera privata[203] e a promuovere le loro competenze mediatiche[204]. Raccomanda altresì la creazione di uno spazio protetto per i bambini in Internet, che dovrebbe essere realizzato grazie all'introduzione di un marchio paneuropeo a garanzia dei sistemi responsabili di certificazione per i contenuti online[205]

Anche la proposta UE di regolamento generale sulla protezione dei dati [206] contiene disposizioni specifiche per la tutela dei bambini. Ai fini del presente regolamento, per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali di minori di età inferiore ai tredici anni è lecito se e nella misura in cui il consenso è espresso o autorizzato dal genitore o dal tutore del minore[207]. Conformemente all'articolo 11 il responsabile del trattamento fornisce all'interessato tutte le informazioni e le comunicazioni relative al trattamento dei dati personali in forma intelligibile, con linguaggio semplice e chiaro e adeguato all'interessato, in particolare se le informazioni sono destinate ai minori.

Con il programma «Internet più sicuro» 2009-2013[208] l'UE promuove la sensibilizzazione del pubblico, la creazione di punti di contatto che consentano di segnalare i contenuti illeciti o dannosi (adescamento dei minori su Internet, bullismo su Internet, ecc.), iniziative di autoregolamentazione e la partecipazione dei bambini alla creazione di un ambiente online più sicuro, nonché la creazione di una base di

---

[202] Stando allo studio EU Kids Online 2011 il 27% dei ragazzi dai 9 ai 12 anni non indicano la loro vera età sulle reti sociali e il 38% dei ragazzi dai 9 ai 12 anni ha un profilo su una rete sociale. Vedi, EU Kids Online Final Report, settembre 2011, pag. 18.

[203] Déclaration sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur l'Internet.

[204] Raccomandazione Rec(2006)12 relativa alla responsabilizzazione dei bambini nel nuovo contesto dell'informazione e della comunicazione,

[205] Raccomandazione CM/Rec(2009)5 sulla protezione dei bambini contro i contenuti e i comportamenti pregiudizievoli per promuovere la loro partecipazione attiva nei nuovi sistemi di informazione e comunicazione.

[206] Proposta di regolamento generale sulla protezione dei dati, COM(2012) 11 definitivo. In merito agli sforzi dell'UE relativi alla tutela dei bambini cfr. anche la comunicazione della Commissione "Strategia europea per un'internet migliore per i ragazzi", COM(2012) 196 definitivo, contenente estese richieste e raccomandazioni della Commissione.

[207] Vedi articolo 8 Proposta di regolamento generale sulla protezione dei dati, COM(2012) 11 definitivo.

[208] Decisione n. 1351/2008/CE del Parlamento europeo e del Consiglio, del 16 dicembre 2008 , relativa a un programma comunitario pluriennale per la protezione dei bambini che usano Internet e altre tecnologie di comunicazione, GU L 348 del 24.12.2008, pag. 118–127.

conoscenze comprendente le nuove tendenze nell'utilizzo delle tecnologie online e le loro conseguenze per la vita quotidiana dei bambini[209].

Parte del programma è dedicata alla promozione *dell'autoregolamentazione del settore Internet*. In quest'ambito nel 2009 le principali reti sociali attive in Europa hanno firmato i «Safer Social Networking Principles for the EU»[210]. Questi principi prevedono tra l'altro che i profili utente dei bambini vengano impostati automaticamente come privati e che siano previsti meccanismi di segnalazione e di cancellazione efficaci per i contenuti problematici e le richieste di contatto. Inoltre, vanno proposte informazioni facilmente comprensibili sulla sicurezza e la sfera privata nelle reti sociali nonché buone impostazioni per la sfera privata. Va bloccata anche la richiesta di contatto con i bambini da parte di estranei e i profili utente dei bambini non devono essere accessibili tramite i motori di ricerca.

4.6.1.3 Situazione legale in Svizzera

Le prescrizioni legali generali descritte nel rapporto, intese a proteggere dai rischi nelle reti sociali, come ad esempio il diritto sulla protezione dei dati o quella della personalità iscritta nel Codice civile e nel Codice penale, sono rivolte anche ai bambini e ai giovani. Per i bambini sono particolarmente importanti gli strumenti di protezione contro il bullismo su Internet e l'adescamento di minori su Internet (cfr. punto 4.4.2), il furto d'identità (cfr. punto 4.4.3.), la pornografia (cfr. punto 4.5.2) come pure i rischi per la salute trattati nel presente rapporto (cfr. punto 4.5.4).

Oltre a queste misure generali di protezione l'ordinamento giuridico svizzero contiene anche numerose disposizioni che si rivolgono appositamente alla tutela e al sostegno di bambini e giovani. I bisogni particolari dei bambini sono difesi nella Costituzione federale e in diversi trattati internazionali vincolanti per la Svizzera[211]. A livello di legge e di ordinanza sono previste misure di tutela particolari ad esempio nel diritto penale[212], nel diritto civile[213], nell'ordinamento radiotelevisivo[214], nel diritto del lavoro[215] o nella regolamentazione sulle derrate alimentari (consegna di alcool)[216]. Il legislatore federale si è impegnato anche nell'ambito del sostegno ai giovani[217].

Finora il diritto federale non prevede disposizioni di protezione della gioventù appositamente orientate alla regolamentazione delle reti sociali. Alcune prescrizioni a tutela dei bambini e dei giovani si esten-

---

[209] Cfr. http://europa.eu/legislation_summaries/information_society/internet/l24190d_it e la comunicazione della Commissione "Valutazione intermedia del programma pluriennale dell'Unione per la protezione dei minori che usano internet e le altre tecnologie di comunicazione", COM(2012) 33 definitivo.

[210] I link verso i "Safer Social Networking Principles" e i rapporti d'attuazione della Commissione UE sono consultabili all'indirizzo: http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm. Un altro accordo di autoregolamentazione a livello UE è la "CEO Coalition to make the Internet a better place for kids" fondata nel dicembre 2011, documenti di fondo e informazioni sull'accordo si trovano all'indirizzo Internet: http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm (sito in lingua inglese).

[211] Cfr. art. 11, 19, 41, 62, 67, 123b Cost. Nel campo dei trattati internazionali si veda ad. es la Convenzione del 20.11.1989 sui diritti del fanciullo, RS **0.107**, compresi i protocolli facoltativi, o la Convenzione n. 182 del 17 giugno 1999 concernente il divieto delle forme più manifeste di sfruttamento del fanciullo sul lavoro e l'azione immediata volta alla loro abolizione, RS **0.822.728.2**. La Convenzione del Consiglio d'Europa del 25.10.2007 sulla protezione dei minori contro lo sfruttamento e l'abuso sessuali è stata approvata dal Consiglio federale e dall'Assemblea federale; vedi FF **2012** 6761 e FF **2012** 6837.

[212] Art. 5, 136, 187, 188, 195, 197, 213, 219, 220, 363 seg., 264 seg. CP; legge federale del 20 giugno 2003 sul diritto penale minorile (DPMin), RS **311.1**; legge federale del 20 marzo 2009 di diritto processuale penale minorile (PPMin), RS 312.1.

[213] Art. 296 segg., 307-317 CP.

[214] Art. 5, 13 LRTV e art. 4, 16 ORTV.

[215] Ordinanza 5 del 28 settembre 2007 concernente la legge sul lavoro (OLL 5), RS **822.115**; ordinanza del DEFR del 4 dicembre 2007 sui lavori pericolosi per i giovani, RS **822.115.2**.

[216] Art. 11 ordinanza del 23 novembre 2005 sulle derrate alimentari e gli oggetti d'uso (ODerr), RS **817.02**.

[217] Legge federale del 30.09.2011 30.09.2011 sulla promozione delle attività extrascolastiche di fanciulli e giovani (LPAG), RS **446.1**; Ordinanza del 17 ottobre 2012 sulla promozione delle attività extrascolastiche di fanciulli e giovani (OPAG), RS **446.11**; Ordinanza dell' 11 giugno 2010 sui provvedimenti per la protezione dei fanciulli e dei giovani e il rafforzamento dei diritti del fanciullo, RS **311.039.1**.

dono tuttavia anche alle reti sociali, si pensi al divieto di pubblicizzare tabacco e alcool presso i giovani[218] o al divieto di rendere la pornografia accessibile ai giovani di età inferiore ai 16 anni.

Per proteggere bambini e giovani non è sufficiente mettere a disposizione strumenti giuridici; molto importante è anche il comportamento dei genitori. Nell'ambito della loro autorità parentale possono definire il comportamento dei propri figli nelle reti sociali e con i loro dati personali, nella misura in cui questi ultimi siano incapaci di discernimento per quanto riguarda le loro azioni nelle reti sociali o la loro capacità di discernimento è perlomeno dubbia. La capacità di discernimento di un bambino non può essere definita in modo astratto, ma solo in base a un comportamento concreto[219].

Se le azioni di un bambino capace di discernere coinvolgono i suoi diritti strettamente personali, il potere di rappresentanza dei genitori giunge ai suoi limiti[220]. I bambini capaci di discernimento che non hanno l'esercizio dei diritti civili esercitano in piena autonomia i diritti strettamente personali; sono fatti salvi i casi nei quali la legge prevede il consenso del rappresentante legale (Art. 19c CC). Ciò è significativo per le attività nelle reti sociali, dato che queste toccano regolarmente quei diritti strettamente personali che gli utenti esercitano in piena autonomia. I bambini capaci di discernimento non hanno pertanto bisogno dell'autorizzazione del loro rappresentante legale per pubblicare su reti sociali dati personali su se stessi, come ad esempio foto, o contenuti da loro creati. Inoltre, nel contesto di una lesione della personalità, il consenso del bambino capace di discernimento è fondamentalmente valido (Art. 13 cpv. 1 LPD; art. 28 cpv. 2 CC).[221]

Il programma nazionale «Protezione della gioventù dai rischi dei media e competenze mediali», avviato dal Consiglio federale nel 2012, mira a sensibilizzare bambini e giovani in merito alle opportunità e ai rischi in Internet e a fornire a genitori, insegnanti e altre persone di riferimento misure appropriate per accompagnarli in rete, tenendo conto anche dei media sociali. Il sito web http://www.giovaniemedia.ch/de.html presenta misure tese a sostenere genitori, persone di riferimento e scuole.

Nel 2011, nel suo Rapporto di valutazione sulla protezione dei dati il Consiglio federale ha evocato la prospettiva di verificare misure tese a meglio proteggere i dati dei minori che tengano conto del fatto che, rispetto agli adulti, essi sono meno consapevoli dei rischi ai quali si espongono nel trattamento dei dati personali.[222]

4.6.2 Collaboratori

4.6.2.1 Situazione iniziale

A livello internazionale[223], ma anche in Svizzera[224] si evocano spesso i rischi legati alla pubblicazione di dati personali su reti sociali in vista di future candidature. È risaputo che nelle loro procedure di reclutamento i datori di lavoro sfruttano i motori di ricerca su Internet per informarsi sui potenziali nuovi collaboratori. Spesso gli utenti sono poco consapevoli che le informazioni da loro collocate su una piattaforma possono essere, a seconda di come è impostata la sfera privata, rintracciate da motori di

---

[218] Art. 18 ordinanza del 27.10.2004 sui prodotti del tabacco e gli articoli per fumatori con succedanei del tabacco (OTab), RS 817.06 e art. 4 Ordinanza del DFI del 23 novembre 2005 sulle bevande alcoliche, RS **817.022.110**.

[219] *BSK-ZGB I*, Bigler-Eggenberger Margrith, 4a ed., Basilea 2010, art. 16, pag. 177 seg. n. marg. 14 seg.

[220] *BSK-ZGB I*, Schwenzer Ingeborg, 4a ed., Basilea 2010, art. 304/305, pag. 1606 n, marg. 6.

[221] Rosenthal David/Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 104 n. 70.

[222] Rapporto del Consiglio federale concernente la valutazione della legge federale sulla protezione dei dati, n. 5.2.2 (FF **2012** 240)

[223] Cfr. Parere del Comitato economico e sociale europeo sul tema «Utilizzo responsabile delle reti sociali e prevenzione dei disturbi a queste associati», 2012/C 351/07, pag. 2, 7, 10.

[224] "Schweizer Konzerne überprüfen Bewerber im Internet", Tagesanzeiger del 02.05.2011, http://www.tagesanzeiger.ch/leben/gesellschaft/Schweizer-Konzerne-ueberpruefen-Bewerber-im-Internet/story/17153295?dossier_id=510 .

ricerca esterni. Inoltre, attraverso profili utente di terzi, i datori di lavoro possono procurarsi accesso a informazioni che i candidati rivelano nelle reti sociali.

4.6.2.2 Soluzioni adottate all'estero o nel diritto internazionale

In un progetto di modifica della legge tedesca sulla protezione dei dati ci si occupa di definire il volume di dati autorizzati ad essere rilevati in vista di un rapporto d'impiego (protezione dei dati del candidato)[225]. Con la modifica si intende vietare ai datori di lavoro di rilevare dati sui candidati nelle reti sociali, nonostante questi siano pubblicamente accessibili (ad esempio tramite motori di ricerca esterni). Le reti professionali (si pensi a Xing o LinkedIn) sono escluse dalla regolamentazione. Questa tendenza va seguita soprattutto alla luce dell'attuale revisione del diritto europeo sulla protezione dei dati.

Da febbraio 2013 al Congresso statunitense è sottoposto il progetto di una legge[226] che vieta a datori di lavoro, scuole universitarie e centri di formazione locali di chiedere a collaboratori, candidati, studenti e allievi il nome utente, la password o alte possibilità d'accesso ai loro profili nelle reti sociali o ai loro conti privati di posta elettronica. Le persone coinvolte non devono subire conseguenze negative se rifiutano di comunicare questo tipo di informazioni. In alcuni Stati americani come la California, il Maryland e l'Illinois, prescrizioni di legge analoghe sono già entrate in vigore[227].

4.6.2.3 Situazione legale in Svizzera

La legislazione svizzera non disciplina esplicitamente se e in che misura i datori di lavoro possono attingere dai media sociali informazioni sui candidati. L'articolo 328b CO permette al datore di lavoro di trattare dati riguardanti il collaboratore nella misura in cui concernono la sua attitudine per il rapporto di lavoro o sono necessari alla stipula del contratto di lavoro. Il Tribunale federale e un'ampia fetta della dottrina conferma che la prescrizione si applica alla fase di candidatura prima dell'esistenza di un rapporto di lavoro, vi sono però anche opinioni contrarie[228]. Il tenore della norma stabilisce già una frontiera oggettiva per quanto riguarda i dati che il datore di lavoro può rilevare su un candidato. Profili privati, non professionali nelle reti sociali possono contenere determinate informazioni sull'attitudine del candidato. Generalmente però, i profili privati degli utenti contengono soprattutto informazioni che esulano dal campo d'applicazione dell'articolo 328b CO, infatti le informazioni dell'ambito privato rientrano solo raramente nei dati sull'attitudine del collaboratore[229]. Dato che il datore di lavoro, se richiama questi dati, vede inevitabilmente l'intero contenuto del profilo utente, è più che problematico definire se, conformemente all'articolo 328b CO possa avere il diritto di consultare i profili privati dei candidati. Una parte della dottrina ritiene che una ricerca generale, a orientamento privato, in Internet tramite un motore di ricerca o nelle reti sociali sia contraria all'articolo 328b CO[230].

Se, attraverso un comportamento illecito (ad es. violazione dell'art. 143bis cpv. 1, art. 179^{novies} o art. 181 CPP), un datore di lavoro si procura accesso a un profilo privato d'utente, oltre alle disposizioni di diritto penale, egli viola anche il principio secondo cui i dati personali possono essere trattati soltanto in modo lecito (art. 4 cpv. 1 LPD). I principi della buona fede nonché della riconoscibilità del trattamento dati (art. 4 cpv. 2 e 4 LPD) vietano al datore di lavoro di procurarsi dati di nascosto. Se un profilo

---

[225] Disegno di legge sulla protezione dei dati dei collaboratori, 17/4230.

[226] Social Networking Online Protection Act del 06.02.2013, H.R.537.

[227] "Kalifornien schützt private Online-Kommunikation vor Arbeitgebern und Unis", heise online (02.10.2012), http://www.heise.de/newsticker/meldung/Kalifornien-schuetzt-private-Online-Kommunikation-vor-Arbeitgebern-und-Unis-1721503.html .

[228] Cfr. sentenza del TF 2C del 30 giugno 2008, consid. 6.2. In favore dell'applicazione dell'art. 328b CO nella fase di candidatura: *BSK-OR I*, Portmann Wolfgang, quinta ed., Basilea 2011, art. 328b, pag. 1952 n. marg. 34 segg. e Streiff Ullin/von Kaenel Adrian/Roger Rudolph, *Arbeitsvertrag Praxiskommentar*, settima ed., Zurigo 2012, art. 328b, pag. 580 n. 4. Contro: Rosenthal David/Jöhri Yvonne, *Handkommentar zum Datenschutzgesetz*, Zurigo 2008, pag. 731 n. 25..

[229] *BSK-OR I*, Portmann Wolfgang, quinta ed., Basilea 2011, art. 328b, pag. 1947 n. marg. 8; Streiff Ullin/von Kaenel Adrian/Roger Rudolph, *Arbeitsvertrag Praxiskommentar*, settima ed., Zurigo 2012, art. 328b, pag. 581 seg.. n. 5.

[230] Egli Urs, "Soziale Netzwerke und Arbeitsverhältnis", in: *Jusletter* 17.01.2011, pag. 9 seg. n. marg. 65 segg.; Streiff Ullin/von Kaenel Adrian/Roger Rudolph, *Arbeitsvertrag Praxiskommentar*, settima ed., Zurigo 2012, art. 328b, pag. 597 n. 10.

utente è privato e il suo titolare non ha autorizzato il datore di lavoro ad accedervi, si è in presenza di una violazione dell'articolo 12 capoverso 2 lettera b LPD se questi vi accede ugualmente. Nel caso in cui un datore di lavoro chieda accesso al profilo privato di un candidato, occorre fondamentalmente mettere in questione la volontarietà del consenso dato dal candidato, visto che potrebbe temere gli effetti negativi di un rifiuto.

Ci si può chiedere in che misura sia giuridicamente limitata la ricerca in Internet da parte del datore di lavoro di dati resi accessibili a tutti (art. 12 cpv. 3 LPD), si pensi ai profili pubblici nelle reti sociali. Si parte dal principio che vi sia una violazione della personalità se un datore di lavoro, in quanto membro di una rete a stampo privato, ricerca in Internet dati pubblicamente accessibili su un candidato che non hanno alcun nesso con la sua attività professionale passata o futura. Se una rete come Facebook fosse incentrata sulla vita privata, allora vi sarebbe un abuso delle informazioni da parte del datore di lavoro se fossero utilizzate per scopi ai quali la persona coinvolta non aveva pensato al momento della pubblicazione[231]. Nella prassi sarà difficile provare se, mediante una semplice ricerca sul web, un datore di lavoro abbia preso visione di dati pubblicamente accessibili. Nelle reti sociali professionali (ad es. XING, LinkedIn) si parte dal principio che l'utente li abbia creati appositamente per essere consultati dai potenziali datori di lavoro[232]. Anche qui però molte informazioni sono accessibili unicamente ai membri della rete.

Per risolvere in modo sensato i problemi che ricorrono in questo contesto, i gestori delle piattaforme dovrebbero proporre sufficienti impostazioni per la sfera privata, i datori di lavoro rispettare in linea di massima la sfera privata dei candidati e gli utenti far prova di autoresponsabilità quando pubblicano dei dati. Nelle sue raccomandazioni in materia di reti sociali, l'Incaricato federale della protezione dei dati e della trasparenza consiglia agli utenti, prima di pubblicare dati personali, di riflettere se in un futuro colloquio d'assunzione desiderano essere confrontati con tali contenuti[233].

4.6.3 Persone disabili

4.6.3.1 Situazione iniziale

Le nuove tecnologie dell'informazione e della comunicazione (TIC), reti sociali comprese, aprono nuovi orizzonti alle persone disabili, infatti esse possono più facilmente partecipare alla vita sociale, informarsi e scambiarsi opinioni. Un presupposto importante è tuttavia l'assenza di barriere in Internet, ovvero la possibilità di accedere a servizi d'informazioni, comunicazione e transazione offerti in Internet.

4.6.3.2 Soluzioni adottate all'estero o nel diritto internazionale

Le raccomandazioni a livello internazionale (Web Content Accessibility Guidelines WCAG 2.0 del Consorzio World Wide Web) mirano a garantire l'accessibilità delle TIC per le persone disabili[234]. Anche la Raccomandazione CM/rec(2012)4 del Consiglio europeo sulla protezione dei diritti dell'uomo nelle reti sociali invita i gestori di reti sociali a garantire l'accessibilità dei loro servizi ai disabili.

4.6.3.3 Situazione legale in Svizzera

In Svizzera vi è un obbligo legale per le collettività pubbliche, di mettere a disposizione, nel limite della proporzionalità, media sociali senza barriere. Ciò risulta dal divieto di discriminazione sancito all'articolo 8 capoverso 2 della Costituzione e, per la Confederazione in particolare, dalla legge sui disabili[235],

---

[231] Cfr. Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: *Jusletter* 17.01.2011, n. marg. 66 segg.

[232] Cfr. Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: *Jusletter* 17.01.2011, n. marg. 70 segg

[233] Cfr. http://www.edoeb.admin.ch/themen/00794/01124/01254/01831/index.html?lang=de

[234] http://www.w3.org/TR/WCAG/ .

[235] Legge federale del 13 dicembre 2002 sull'eliminazione di svantaggi nei confronti dei disabili (LDis), RS **151.3**.

nel cui campo d'applicazione rientrano anche le prestazioni via Internet[236]. Conformemente all'articolo 6 LDis, ai fornitori privati di prestazioni, fruibili in linea di massima da tutti, è soltanto vietato discriminare i disabili a causa del loro handicap. Non se ne deduce quindi un obbligo di mettere a disposizione prestazioni in Internet senza barriere.

In considerazione dell'importanza che i media sociali hanno acquisito sia in generale, sia per quanto riguarda l'inclusione delle persone disabili nella vita sociale, la garanzia di un accesso senza barriere alle prestazioni offerte sui media sociali è più che auspicabile. Misure legislative introdotte a livello nazionale avrebbero però pochissimo effetto sui media sociali più utilizzati. Sembra tuttavia sensato collaborare con attori centrali per cercare di influire con altre misure sul rispetto degli standard di accessibilità.

4.7 Postulato Amherd 12.3545 «Accesso a Facebook per i più giovani»

Il postulato 12.3545[237] incarica il Consiglio federale di valutare le misure atte a proteggere i bambini in Svizzera dai rischi legati ai media sociali. Oltre agli eventuali adeguamenti legali vanno anche indicati i possibili provvedimenti a sostegno di genitori, incaricati dell'educazione e scuole. Il Consiglio federale è segnatamente chiamato a esaminare l'opportunità di collegare fra loro i conti Facebook dei figli e dei genitori, e il potenziale dei certificati d'identità elettronici come la Suisse ID in questo contesto. Stando ai sondaggi, in Svizzera sono pochi i bambini minori di 13 anni che hanno un profilo su una piattaforma sociale. [238]

L'intenzione di Facebook di abbassare il limite d'età degli utenti a 13 anni e di collegare i profili dei minori di 13 anni con quelli dei loro genitori, potrebbe essere dettata da un interesse pecuniario, infatti permetterebbe di acquisire un nuovo gruppo di clienti, interessante soprattutto per il mercato dei giochi, in piena espansione e pubblicizzato su Facebook. Il collegamento al profilo dei genitori potrebbe, in caso di stipula del contratto da parte dei figli, implicare il consenso (tacito o esplicito) dei genitori. D'altra parte è immaginabile che Facebook intenda anticipare di sua iniziativa una regolamentazione statale allo scopo di rendere poi questa obsoleta.[239]

Come già descritto al punto 4.6.1.3, le prescrizioni giuridiche generali sulla protezione dai rischi dei media sociali sono rivolte anche a bambini e giovani. Vigono inoltre numerose disposizioni specifiche per la tutela e la promozione di bambini e giovani, che si applicano anche nei media sociali.

Collegare i profili dei figli a quelli dei genitori pone diversi problemi. Presuppone infatti che anche i genitori abbiano un profilo su questa piattaforma e lo gestiscano. Una condizione certo vantaggiosa per la piattaforma in questione ma probabilmente rifiutata da molti genitori che per un motivo o un altro non desiderano utilizzarla. Inoltre, il collegamento dei profili di genitori e figli potrebbe limitare i diritti della personalità dei bambini capaci di discernimento.

Affinché sia possibile introdurre un controllo elettronico standardizzato per determinare l'età su una piattaforma di media sociali, quest'ultima dovrebbe creare i presupposti nel sistema e verificare di volta in volta le identità. Attualmente non è possibile sapere se SuisseID soddisferebbe i requisiti di Facebook in tale contesto.

---

[236] Secondo l'art. 10 dell'ordinanza del 19 novembre 2003 sull'eliminazione di svantaggi nei confronti dei disabili (ODis), RS **151.3.1**, tutte le prestazioni su Internet e i media sociali della Confederazione devono essere accessibili alle persone disabili. Lo standard di riferimento per i siti della Confederazione è dato dalla Norma P028 - "Direttive della Confederazione per l'allestimento di siti Internet senza barriere". Cfr. http://www.isb.admin.ch/themen/standards/alle/03237/ (sito in francese e tedesco).

[237] http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20123545

[238] Hans Bredow-Institut, *Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen an den Jugendmedienschutz, Entwurf des Endberichts*, 2013, n. 1.4, pag. 27; in Germania problema sembra essere più accentuato, infatti si registra un'età media di 12,7 anni al momento della prima registrazione del profilo: Caspar Johannes, "Soziale Netzwerke und Einwilligung der Nutzer", in: *digma* 2013, pag. 62.

[239] Si veda ad es. http://online.wsj.com/article/SB10001424052702303506404577444711741019238.html#

4.8 Tentativo di un apprezzamento complessivo dell'attuale situazione legale

Le regolamentazioni giuridiche descritte nel presente capitolo 4 per le varie questioni giuridiche sollevate dai media sociali, presentano un quadro particolarmente variegato. È difficile fare affermazioni generali, detto in parole povere e stando alle esperienze fatte finora, le regolamentazioni del diritto giuridico svizzero, spesso formulate in modo aperto, possono, in caso di conflitto, essere interpretate e applicate in modo da giungere a soluzioni eque: non saltano all'occhio grandi lacune regolamentari.

Finora i tribunali e le amministrazioni svizzera hanno dovuto confrontarsi raramente con questi problemi. Ci si chiede infatti se il diritto vigente crei sufficienti incentivi per i diretti interessati a difendere attivamente i propri diritti. Potenziale di miglioramento potrebbe, ad esempio, trovarsi in diversi aspetti inerenti la protezione dei dati (si pensi alle risorse dell'IFPD e all'assenza dell'obbligo di creare impostazioni favorevoli alla protezione dei dati; cfr. punto 4.3.1.5). L'evoluzione tecnica potrebbe contribuire a rendere più attenta la popolazione alle pretese che si possono avanzare sulla base del diritto vigente.

Inoltre, in molti ambiti rimane una certa insicurezza riguardo al fatto se in un conflitto disputatosi in tribunale le prescrizioni generali applicate alle nuove questioni giuridiche portino effettivamente a risultati soddisfacenti. Questa insicurezza è, non da ultimo, legata al fatto che in un ambiente internazionale come quello delle piattaforme sociali, l'applicazione pratica delle pretese giuridiche attuali può essere precaria.

5 Problema di fondo: l'applicazione del diritto

5.1 In generale

In relazione alle singole fattispecie, il capitolo 4 esamina se il diritto svizzero applicabile (in particolare LPD, CC, LCSI e CP) risponda in modo appropriato ai problemi giuridici che pongono specificatamente le reti sociali.

In questa sede si approfondirà il problema dell'applicazione del diritto, un argomento di importanza focale poiché i responsabili di violazioni di legge (ad es. gli autori di contenuti illeciti su una piattaforma sociale) spesso non possono essere chiamati a risponderne. Occorre pertanto interrogarsi se il diritto svizzero vigente definisca in modo sufficientemente chiaro le responsabilità delle parti coinvolte.

Inoltre, i gestori delle reti sociali sono spesso attivi a livello internazionale e pertanto la legislazione nazionale giunge per forza ai suoi limiti.

5.2 Perseguimento penale degli autori di contenuti illeciti diffusi su piattaforme sociali

5.2.1 Il problema dell'anonimato

Come esposto nel capitolo 4, i contenuti pubblicati su piattaforme sociali possono violare una lunga serie di disposizioni di diritto penale (ad es. diffamazione, pornografia, discriminazione razziale e pubblica istigazione a un crimine o alla violenza) o di diritto civile (ad es. protezione della personalità). Nella pratica, l'applicazione di queste disposizioni incontra spesso degli ostacoli. Infatti, gli autori di eventuali contenuti illeciti possono essere chiamati a rispondere solo qualora sia nota la loro identità, alla quale tuttavia non sempre si riesce a risalire vista la tendenza diffusa a pubblicare contenuti in forma anonima (o sotto pseudonimo) su blog o piattaforme come Facebook. L'individuazione univoca del responsabile risulta in questi casi difficile, se non praticamente impossibile.
Le autorità svizzere preposte al perseguimento penale possono tuttavia seguire una o l'altra pista, in particolare mediante l'accesso ai cosiddetti indirizzi IP, ossia le etichette numeriche che identificano un dispositivo collegato a una rete informatica, che l'utente normalmente non vede ma che i gestori di rete generalmente registrano se un utente utilizza una piattaforma di media sociali o invia un'e-mail. La possibilità e l'autorizzazione di accedere a questi indirizzi dipende anche dal gestore della piattaforma in questione.

5.2.2 Contributi anonimi su piattaforme di media professionisti

L'ordinamento giuridico riconosce da diverso tempo che le pubblicazioni anonime non sono sistematicamente riconducibili a motivi di natura deplorevole.[240] Il Codice penale tutela, persino in modo esplicito, la pubblicazione anonima su ampia scala. Secondo l'articolo 28*a* del Codice penale e l'articolo 172 del Codice di procedura penale, tutte le persone che si occupano professionalmente della pubblicazione di informazioni nella parte redazionale di un periodico non sono autorizzate a rivelare l'identità dell'autore. Le medesime e i loro ausiliari hanno diritto a non trasmettere alle autorità preposte al perseguimento penale gli indirizzi IP di autori anonimi. Tale diritto si applica anche alle piattaforme sociali, fra cui i blog, qualora siano gestite da media professionisti. In virtù di questa disposizione, il Tribunale federale ha accettato il rifiuto della SSR di fornire al pubblico ministero del Cantone di Zugo l'indirizzo IP di una persona presumibilmente responsabile di avere pubblicato sotto falso nome commenti lesivi dell'onore nel blog della SSR relativo alla trasmissione televisiva «Alpenfestung».[241] Qualora l'autore della violazione non possa essere individuato o tradotto dinnanzi a un tribunale svizzero, è punito il redattore responsabile (o, in sua mancanza, la persona responsabile della pubblicazione) per mancata opposizione a una pubblicazione punibile (art. 322bis CP).

5.2.3 Contributi anonimi su altre piattaforme

Diversa è la situazione che riguarda i gestori di piattaforme non attivi quali media professionisti. Questi ultimi potrebbero, infatti, essere obbligati dalle autorità competenti a rivelare gli indirizzi IP di persone sospette. I rispettivi dati devono essere (stati) memorizzati in conformità alla legge federale sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT; RS *780.1*). La LSCPT obbliga sia gli offerenti di prestazioni di telecomunicazione sia gli offerenti Internet (art. 1 cpv. 2) a conservare per un periodo di sei mesi i dati necessari all'identificazione degli utenti, come anche i dati relativi al traffico e alla fatturazione (art. 15 cpv. 3) e di trasmetterli su richiesta al servizio preposto alla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (art. 15 cpv. 1). Conformemente alla prassi attuale e al tenore dell'articolo 1 in italiano e francese, l'obbligo incombe solamente sui fornitori di accessi Internet. I gestori delle piattaforme sono tenuti a rivelare unicamente i dati a loro disponibili. In virtù dell'articolo 22 capoverso 4 del disegno di revisione della LSCPT [242], il Consiglio federale può obbligare alla conservazione dei dati i fornitori di servizi che si fondano su prestazioni di telecomunicazione e permettono una comunicazione unilaterale o multilaterale (fornitori di servizi di comunicazione derivati, come per esempio gli FST). Nel caso di un atto illecito commesso su Internet, il diritto vigente autorizza le autorità preposte al perseguimento penale a far luce sull'identità del proprietario del collegamento coinvolto anche senza decisione giudiziaria e a procedere, per esempio, alla perquisizione del suo domicilio. Per questo motivo, il Tribunale federale ha confermato nel 2010 la pena inflitta per favoreggiamento (art. 305 CP) a un gestore di una piattaforma Internet, ritenuto responsabile di avere distrutto, in qualità di fornitore di servizi Internet, gli indirizzi IP di autori anonimi di presunti contenuti lesivi dell'onore, permettendo loro di sottrarsi al perseguimento penale.[243]

L'applicazione della legislazione vigente risulta più difficile quando gli indirizzi IP sono noti unicamente al gestore di una piattaforma estera non sottoposta alle disposizioni della LSCPT. In tal caso, le autorità svizzere devono appellarsi alla collaborazione del gestore estero o seguire altrimenti la via spinosa dell'assistenza internazionale in materia penale. I gestori esteri di una piattaforma non sono sempre disposti a rimuovere un contenuto, ma talvolta acconsentono, solo a determinate condizioni, a trasmettere alle autorità preposte al perseguimento penale, previa richiesta, l'indirizzo IP di una persona responsabile di avere pubblicato per esempio un'affermazione illecita.

---

[240] Si veda ad es. DTF 55 II 94 consid. 1 pag. 98.

[241] DTF 136 IV 145.

[242] FF **2013** 2383.

[243] Sentenza del Tribunale federale 6B_766/2009 dell'8.1.2010.

5.2.4 Competenza territoriale

Nel caso delle piattaforme sociali, occorre in primo luogo designare l'autorità competente in materia di perseguimento penale, il che solleva alcuni problemi pratici. Soltanto a conclusione di questa procedura si potrà presentare richiesta di assistenza internazionale (ad es. nel caso di Facebook) e quindi far luce su eventuali violazioni penali. Considerato che le affermazioni pubblicate su piattaforme internazionali sono accessibili da qualsiasi luogo, sussiste il rischio che né il Ministero pubblico cantonale né il Ministero pubblico della Confederazione siano dichiarati competenti per l'avvio del procedimento giuridico. Pertanto l'articolo 27 capoverso 2 del Codice di procedura penale consente al Ministero pubblico della Confederazione di svolgere le indagini preliminari nel caso in cui l'autorità competente non sia chiara. Se il Ministero pubblico della Confederazione applica questa disposizione in modo coerente, gli atti illeciti commessi su piattaforme sociali possono essere oggetto di un perseguimento penale.

5.3 Responsabilità dei gestori delle piattaforme e dei fornitori di servizi Internet

5.3.1 Soluzioni adottate all'estero o nel diritto internazionale

All'interno dell'Unione europea, la responsabilità dei fornitori di servizi Internet (*provider*) è definita dalle disposizioni specifiche di cui alla direttiva sul *commercio elettronico* [244]: l'articolo 12 di questa direttiva statuisce il principio secondo cui i fornitori di accessi Internet o di semplice trasporto (mere conduit) non possono essere ritenuti responsabili delle informazioni da loro trasmesse. Secondo l'articolo 14 della stessa direttiva anche i fornitori che memorizzano contenuti di terzi sui loro sistemi operativi (*hosting provider*) sono esclusi da qualsiasi responsabilità a condizione che non siano al corrente dell'attività illecita. In caso contrario, saranno tenuti a rimuovere i contenuti in questione o a disabilitarne l'accesso.

Non esiste tuttavia alcun obbligo generale di sorvegliare le informazioni trasmesse o memorizzate, né di ricercare attivamente la presenza di contenuti illeciti (art. 15 direttiva sul commercio elettronico). Anche la Corte di giustizia dell'Unione europea (CGUE) ha riconosciuto che i fornitori di servizi Internet non sono tenuti a sorvegliare sistematicamente tutte le informazioni che memorizzano o rendono accessibili. La CGUE non ha imposto né ai fornitori di servizi d'accesso[245] né ai fornitori di servizi di hosting[246]l'obbligo generale a un filtraggio preliminare.

Tuttavia, se il fornitore non si limita al trattamento automatico dei contenuti pubblicati dai suoi clienti, ma decide di selezionarli o modificarli, allora perde il privilegio garantito dall'articolo 15 capoverso 1 della direttiva sul commercio elettronico relativo all'esenzione dall'obbligo generale di sorveglianza e all'esclusione della responsabilità.[247] Il gestore della piattaforma non svolge un ruolo attivo nel senso indicato se memorizza le offerte sul proprio server, stabilisce le modalità del suo servizio, viene ricompensato per quest'ultimo e fornisce informazioni di ordine generale ai propri clienti. Per contro, la CGUE riconosce che si è in presenza di un ruolo attivo quando il gestore della piattaforma provvede per esempio a ottimizzare la presentazione di un contenuto o a pubblicizzare quest'ultimo. [248]

Sotto il profilo dei diritti dell'uomo, suscita controversie la questione di stabilire se e in quale misura un gestore di una piattaforma debba essere perseguito civilmente per contenuti illeciti (ad es. lesivi della

---

[244] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (Direttiva sul commercio elettronico), GU L 178 del 17.7.2000, pag. 1.

[245] Sentenza CGUE del 24.11.2011, SABAM / Scarlet Extended, causa C-70/10 (ordine a un fornitore di accessi Internet di filtrare e bloccare i file condivisi che violano il diritto europeo).

[246] Sentenza CGUE del 16.2.2012, SABAM / Netlog NV, causa C-360/10 (nessun obbligo in capo al fornitore di servizi di hosting per la generale sorveglianza delle informazioni memorizzate su una piattaforma per reti sociali e per la predisposizione di un sistema di filtraggio atto a impedire violazioni dei diritti d'autore).

[247] Sentenza CGUE del 19.7.2011, L'Oréal / E-Bay, causa C-324/09, Racc. I-6011 (responsabilità del fornitore per avere svolto un "ruolo attivo").

[248] Sentenza CGUE del 19.7.2011, L'Oréal / E-Bay, causa C-324/09, Racc. I-6011 n. marg. 115 seg.

personalità) pubblicati dai suoi utenti, e condannato al pagamento di una somma di denaro a titolo di riparazione morale. Presso la Corte europea dei diritti dell'uomo è tuttora pendente il ricorso presentato nel 2009 da un gestore estone di un portale d'informazione condannato per violazione della libertà di espressione (art. 10 CEDU). [249]

5.3.2 Situazione legale in Svizzera

Come all'estero, anche in Svizzera è un fatto indiscusso che gli autori di contenuti illeciti pubblicati su piattaforme di media sociali (fornitori di contenuto) possano essere ritenuti giuridicamente responsabili qualora siano identificati e tradotti in giudizio. Diversamente dalla maggior parte degli Stati membri dell'Unione europea, la Svizzera non prevede alcuna disposizione specifica concernente la responsabilità riferibile ad altri attori implicati nella catena di comunicazione (ad es. fornitori di servizi d'accesso o di hosting). In tale contesto sono determinanti le prescrizioni generali in materia di responsabilità civile e penale. Il rifiuto di un apposito disciplinamento ha suscitato diverse critiche, poiché una scelta simile comprometterebbe la chiarezza richiesta a livello legislativo. Per questa ragione, nel 2001 il Consiglio nazionale e il Consiglio degli Stati hanno richiesto un quadro giuridico atto a garantire la certezza del diritto e hanno trasmesso una mozione in tal senso.

Su tale scia è stata istituita la commissione peritale «Criminalità in rete». Sulla base del rapporto steso da quest'ultima, nel 2004 il Consiglio federale ha posto in consultazione l'avamprogetto concernente la modifica del Codice penale (CP), in particolare del Codice penale militare (CPM). Nonostante sia stato accolto favorevolmente un disciplinamento esplicito della responsabilità penale dei fornitori di servizi Internet e dei gestori dei motori di ricerca, sono emerse controversie su vari aspetti. Nel 2008, il Consiglio federale ha rinunciato a un disciplinamento in materia.

Successivamente, il Consiglio federale ha ribadito a più riprese l'inopportunità di disposizioni specifiche sulla responsabilità dei fornitori di servizi d'accesso e di hosting nel diritto sia penale che civile (si veda mozione Riklin 08.418 «Criminalità in rete. Migliorare la certezza del diritto» e l'interpellanza Stöckli 12.4202 «Swisscom e i contenuti protetti dal diritto d'autore»):

In materia *penale*, il Consiglio federale ritiene che esistano delle soluzioni appropriate al caso, che si fondano sulla punibilità dei mass media (art. 28 CP) e sui principi generali disciplinanti la partecipazione e la complicità (art. 24 segg. CP).

In materia *civile*, i fornitori dei servizi Internet sono responsabili secondo gli stessi principi validi per i fornitori di altri servizi. Conformemente al Codice delle obbligazioni (CO), chiunque è tenuto a riparare il danno illecitamente cagionato a terzi sia con intenzione, sia per negligenza o imprudenza (art. 41 cpv. 1 CO)[250].

Non è stata ancora fatta chiarezza sulla responsabilità in capo ai gestori di piattaforme di media sociali che non rientrano nelle consuete categorie di fornitori.[251]In linea generale, i gestori di piattaforme, rispetto ai fornitori di servizi di hosting, svolgono un ruolo più attivo e possiedono un collegamento più diretto ai contenuti trasmessi. I fornitori di servizi di hosting, infatti, consentono ai propri utenti unicamente il caricamento automatico di informazioni sul server web e mettono a disposizione solo spazio di memoria. I gestori di piattaforme definiscono le regole in materia di allestimento, volume e contenuto delle informazioni prodotte dagli utenti. Diversamente dai tradizionali fornitori di servizi di hosting, sono spesso in grado di esercitare una funzione di sorveglianza e, se necessario, di opporsi alla pub-

---

[249] Ricorso n° 64569/09 «Delfi AS c Estland»; l'11 febbraio 2011, la Corte di giustizia ha sottoposto la questione al parere del governo estone.

[250] Parere del Consiglio federale del 5.3.2010 in risposta alla mozione 09.4222 «Responsabilità giuridica dei fornitori d'accesso alla rete».

[251] Bianchi della Porta Manuel/Robert Vincent, «Responsabilité pénale de l'éditeur de médias en ligne participatifs», in: *medialex* 2009, pag. 21 seg.

blicazione di contenuti controversi. Nel loro caso, la rinuncia ad effettuare una certa operazione di filtraggio attraverso quantomeno controlli a campione o a opporsi tempestivamente a contenuti ritenuti illeciti, ha più possibilità di produrre conseguenze sia civili che penali. L'estensione dei loro obblighi è stata finora semplicemente abbozzata da giudici ed esperti di diritto[252].

In presenza di reati di opinione, è discutibile se e in quale misura i gestori delle piattaforme siano soggetti alle disposizioni speciali in materia di punibilità dei mass media (art. 28 CP) e se, eventualmente, sia attribuita loro una responsabilità sussidiaria per mancata opposizione a una pubblicazione punibile (art. 322bis CP). Uno dei problemi esistenti risiede nel fatto che molte piattaforme diffondono informazioni sia destinate al grande pubblico sia di carattere privato. Le disposizioni vigenti in materia di punibilità dei mass media non sono concepite per tali forme miste. Diversamente dagli editori, dalle emittenti radiofoniche e dai gestori di un singolo sito Internet, i gestori di reti sociali non sono considerati imprese mediatiche nel senso convenzionale del termine.

Secondo la letteratura giuridica, la disposizione speciale (art. 28 CP) concernente la punibilità dei mass media emanata all'epoca della stampa scritta non appare più in grado di rispondere alle esigenze attuali del mondo virtuale. Il suo campo di applicazione nel caso di diversi reati (ad es. pornografia leggera) o dei contenuti pubblicati nei vari mezzi di comunicazione sociale su Internet non ha contorni ben definiti. Le soglie di punibilità dovranno essere pertanto precisate nell'ambito della revisione di legge.[253]

Il Consiglio federale è consapevole che l'esistenza di disposizioni giuridiche chiare vadano a beneficio dei fornitori, dei clienti, delle autorità, ma anche della giustizia. Tuttavia, visto il numero elevato degli attori coinvolti e dei problemi sollevati, qualsiasi progetto di legge concernente la responsabilità dei fornitori di servizi Internet e il perseguimento delle violazioni commesse in rete si confronterà con la sfida di elaborare soluzioni che soddisfino tutte le esigenze. In tale contesto si può correre il rischio di un disciplinamento eccessivo o, al contrario, insufficiente.

Nella sua risposta ad alcuni interventi parlamentari attuali (la mozione Riklin 13.3215 «Disciplinare la responsabilità giuridica dei provider Internet» e la domanda Glättli 13.5059 «Responsabilità degli hosting-provider e dei gestori di blog e forum»), il Consiglio federale ha riconosciuto la necessità di legiferare in materia civile: il Tribunale federale si è nel frattempo occupato, per la prima volta, della responsabilità civile dei fornitori di servizi di hosting in relazione a contenuti illeciti (lesivi della personalità)[254]. Nel quadro di un'azione di cancellazione e accertamento, ha negato il privilegio di esclusione della responsabilità a un fornitore che mette blog di terzi a disposizione sul proprio server. Considerata la mancanza di una disposizione specifica in materia, in Svizzera si applicano le norme generali di cui all'articolo 28 CC.[255] Non spetta alla giustizia, ma al legislatore far fronte alle eventuali conseguenze inattese derivanti da questa situazione legale.[256] A tal riguardo, il Tribunale federale ha rinviato espressamente al presente rapporto, all'epoca ancora in corso di elaborazione.

L'attuale giurisprudenza richiama l'attenzione sul fatto che la giustizia considera insufficienti le disposizioni generali in materia di responsabilità civile e auspica in tale ambito un chiarimento da parte del legislatore. Le opinioni espresse da giudici ed esperti di diritto[257] nonché gli sviluppi internazionali[258]

---

[252] cfr. sempre Bianchi della Porta Manuel/Robert Vincent, «Responsabilité pénale de l'éditeur de médias en ligne participatifs», in: *medialex* 2009, pag. 19 segg.

[253] Christian Schwarzenegger, Der Anwendungsbereich des Medienstrafrechts (Art. 28, 322bis StGB), in: Cavallo (ed.), FS-Donatsch, Zurigo 2012, pag. 187.

[254] Sentenza 5A_792/2011 del 14 gennaio 2013.

[255] Sentenza 5A_792/2011 del 14 gennaio 2013, consid. 6.1.

[256] Sentenza 5A_792/2011 del 14 gennaio 2013, consid. 6.3.

[257] Kernen Alexander, «Volle Verantwortlichkeit des Host Providers für persönlichkeitsverletzende Handlungen seines Kunden», in: *Jusletter* 4 marzo 2013, n. marg. 20 segg.; Bühlmann Lukas, «Blog-Hoster sind mitverantwortlich für persönlichkeitsverletzende Blogbeiträge», in: *Digitaler Rechtsprechungs-Kommentar Weblaw*, 13 marzo 2013, n. marg. 10 seg.; Schoch Nik /

stanno a indicare che occorre esaminare più da vicino la necessità di legiferare in materia civile. Il Consiglio federale si dichiara disposto a compiere passi in tal senso (si veda punto 7.2.4 di cui sotto).

5.4 Decisioni in materia di cancellazione o blocco di contenuti illeciti

5.4.1 Cancellazione di contenuti problematici da una piattaforma

Qualora un contenuto illecito pubblicato su una piattaforma di media sociali presenti un qualsiasi collegamento con la Svizzera, l'autorità preposta al perseguimento penale ha facoltà di intervenire affinché il contenuto contestato sia rimosso. A livello giuridico, può applicare le disposizioni relative al sequestro (art. 263 CPP), fermo restando che il contenuto in questione serva come mezzo di prova nel quadro di un procedimento penale o sia confiscato in altro modo. In virtù dell'articolo 13*e* della legge federale sulle misure per la salvaguardia della sicurezza interna (RS *120*), il fedpol può inoltre ordinare la cancellazione di un sito Internet che diffonde materiale di propaganda istigante alla violenza, se quest'ultimo si trova su un server svizzero. Se invece si dovesse trattare di un server estero, il fedpol può raccomandare al fornitore svizzero di bloccare il sito Internet in questione. Nell'ambito di determinate violazioni delle prescrizioni concernenti la pubblicità (ad es. legge sull'alcool), l'autorità amministrativa competente (ad es. la Regìa federale degli alcool) può favorire l'applicazione della legge mediante una decisione di diritto amministrativo. Anche in tal caso, si possono riscontrare degli ostacoli per quel che concerne contenuti provenienti da piattaforme estere.

In caso di cancellazione, sarà necessario, ove possibile, rimuovere soltanto i contenuti illeciti. I contenuti leciti dovranno invece restare accessibili al fine di evitare un'eccessiva e sproporzionata limitazione della libertà di opinione e d'informazione (art. 16 Cost. e punto 4.2.2 di cui sopra).

Stando all'esperienza dello SCOCI è facile procedere alla rimozione di contenuti illeciti su una piattaforma sociale, come per esempio Facebook, se il fornitore di servizi Internet emette di sua iniziativa un ordine in tale senso. I gestori di reti sociali con sede in Svizzera non sono però ancora riusciti a introdurre un'autoregolamentazione valida per l'intero settore. Anche i gestori tedeschi[259] vi hanno rinunciato in ragione delle implicazioni esistenti a livello transfrontaliero.

Tentativi di elaborare un'autoregolamentazione nel settore si osservano da parte dei fornitori di servizi di hosting, che mettono a disposizione dei gestori di piattaforme (o di altri interessati) spazio di memoria per il caricamento automatico delle loro offerte. Al termine di una fase di lavoro preliminare durata tre anni, nel 2013 molti importanti fornitori svizzeri di servizi di hosting[260] hanno elaborato, sotto l'egida dell'associazione di categoria Simsa, un *Code of Conduct*[261] (codice di condotta) che chiarisce con maggiore precisione il loro ruolo nell'ambito del perseguimento penale di contenuti illeciti pubblicati in rete, oggetto di reati quali pornografia, rappresentazione di atti di cruda violenza, razzismo, lesione dell'onore, ma anche violazioni dei diritti d'autore e della personalità. Se il gestore di un sito Internet o di una rete sociale non può essere identificato, non risponde alle richieste oppure una denuncia nei suoi confronti sembra avere poche possibilità di successo, le persone lese possono sporgere reclamo presso il fornitore di servizi di hosting. Secondo il codice di condotta, quest'ultimo deve trasmettere le accuse formulate al gestore del sito Internet (o della piattaforma) oggetto della contestazione, esortandolo a fare luce sulla situazione e a rimuovere eventuali contenuti di natura illecita. Nei casi eviden-

---

Schüepp Michael, «Provider-Haftung „de près ou de loin“»?, in: *Jusletter* 13 maggio 2013, n. marg. 43 segg.; Hürlimann Daniel, Replik: «Das Leistungsschutzrecht für Presseverlage», in: *Jusletter* 13 maggio 2013, nota a piè di pagina 30.

[258] Per esempio il ricorso n° 64569/09 «Delfi AS c Estland» (nota a piè di pagina * 242) presentato presso la CEDU, concernente l'obbligo del gestore di un portale d'informazione di pagare una riparazione morale per avere diffuso automaticamente contenuti illeciti di terzi (commenti lesivi della personalità).

[259] http://www.heise.de/newsticker/meldung/Selbstregulierung-von-Social-Networks-gescheitert-1857533.html (disponibile solo in tedesco).

[260] Secondo Sisma, in questa categoria rientrano i più importanti fornitori svizzeri di servizi di hosting: Cyon, Green, Hostpoint, Metanet, Nine, Swisscom e Webland.

[261] Code of conduct hosting (CCH); http://static.simsa.ch/1362151411/130201_simsa_cch_public_web.pdf (disponibile solo in inglese).

ti, i fornitori di servizi di hosting possono bloccare in via temporanea l'accesso al sito Internet in questione.

Da alcune indagini condotte in Germania è emerso che i modelli di autoregolamentazione (e di autoregolamentazione diretta dallo Stato), pur presentando alcuni vantaggi rispetto alle forme di regolamentazione statale all'estero, funzionano in modo complesso e instabile. L'autoregolamentazione incontra degli ostacoli specialmente nel caso di fornitori esterni (ad es. esteri) che non fanno parte dell'organizzazione di categoria.[262]

5.4.2 Blocco dell'accesso a contenuti problematici attraverso il fornitore dell'accesso

Qualora la cancellazione di contenuti problematici dalla piattaforma sociale in questione (nella maggior parte dei casi estera) non possa essere effettuata, o effettuata tempestivamente, si prende in esame la possibilità di bloccarne l'accesso. Nell'ambito della pedopornografica o dell'abuso di minori, lo SCOCI mette a disposizione dei fornitori svizzeri una lista di link a siti Internet esteri, che presentano chiaramente contenuti illeciti e che continuano a essere accessibili, malgrado la richiesta di cancellazione presentata alle autorità estere. In virtù delle loro condizioni generali di contratto, i fornitori provvedono a bloccare i contenuti illeciti e a sostituirli con un messaggio di divieto dello SCOCI. Questa forma di collaborazione volontaria tra autorità ed economia privata si è rivelata uno strumento efficace, che permette annualmente di bloccare attraverso i fornitori di servizi Internet centinaia di migliaia di accessi a pagine Internet a contenuto illecito e di tutelare al meglio i diritti delle vittime.

In passato, queste misure di blocco sono state ordinate in casi sporadici dalle autorità svizzere preposte al perseguimento penale; un giudice istruttore del Cantone di Vaud ha optato per tale misura contro contenuti lesivi dell'onore pubblicati sul sito Internet «Appel au peuple».[263] La letteratura giuridica critica il fatto che tali decisioni non dispongano di una base giuridica chiara nella legislazione svizzera.[264]

Occorre tenere ben presente che l'adozione di misure di blocco è suscettibile di provocare danni collaterali ai contenuti leciti bloccati. Infatti, se l'accesso a un certo nome di dominio è bloccato, non sarà più possibile visualizzare tutte le offerte lecite e gradite proposte su questa risorsa.[265] Alla fine del 2012, la Corte europea dei diritti dell'uomo ha contestato in un caso riguardante la Turchia[266] l'ordine di bloccare l'intera piattaforma Google Sites a causa di un singolo sito Internet dal contenuto problematico. Misure di blocco simili necessitano di una base legale sufficientemente precisa. Secondo la Corte, occorre definire il quadro giuridico in modo rigoroso e sottoporre le misure a un controllo efficace da parte delle autorità giudiziarie nazionali, così da impedire decisioni arbitrarie.

Considerate le attuali basi legali e l'efficace collaborazione tra autorità e fornitori di servizi Internet, nella sua risposta all'interrogazione Schwaab (12.1128, Accesso ai contenuti su Internet. Strategia «cancellare invece di bloccare»), il Consiglio federale ha smentito la necessità di elaborare apposite basi legali.

---

[262] Hans Bredow-Institut, *Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen an den Jugendmedienschutz*, Entwurf des Endberichts 2013, punto 2.2.2.1.4. pag. 45.

[263] Si veda il fatto di cui alla sentenza del Tribunale federale 1B_242/2009 del 21.10.2009.

[264] Schwarzenegger Christian, «Sperrverfügungen gegen Access-Provider - über die Zulässigkeit polizeilicher Gefahrenabwehr durch Sperranordnungen im Internet», in: Arter Oliver/Jörg Florian (ed.), *Internet-Recht und Electronic Commerce Law*, Berna 2003, pag. 249 segg.

[265] Rosenthal David, «Internet-Provider-Haftung – ein Sonderfall?» in: Peter Jung (ed.), *Aktuelle Entwicklungen im Haftungsrecht*, Berna/Zurigo/Basilea/Ginevra, 2007, pag. 158.

[266] Sentenza della CEDU «Ahmet Yildirim c. Turchia» (ricorso n°3111/2010) del 18.12.2012 concernente il blocco che viola la convenzione della piattaforma Google Sites.

5.5 Difficoltà nell'applicazione del diritto in contesti transfrontalieri

L'applicazione della legislazione svizzera in materia di reti sociali risulta difficile per due motivi principali: la maggior parte dei gestori delle piattaforme incriminate risiedono all'estero e la forma di comunicazione privilegiata è generalmente di natura transfrontaliera. In molti ambiti, il diritto svizzero prevede un disciplinamento relativo ai problemi sollevati dai media sociali, che spesso potrebbe essere applicato anche ai casi transfrontalieri. Non è tuttavia garantito che una sentenza definitiva emessa da un tribunale svizzero possa essere eseguita anche all'estero.

5.5.1 Applicazione del diritto da parte delle autorità preposte all'istruttoria e al perseguimento penale

5.5.1.1 Cooperazione internazionale

Nella prassi, l'applicazione del diritto dipende in misura preponderante dalla disponibilità a collaborare del gestore della piattaforma (estera). L'invito a collaborare può essere rivolto dalle autorità preposte al perseguimento penale. Per questa ragione alcuni gestori di piattaforme di media sociali hanno creato dei servizi ai quali alcune autorità estere possono rivolgersi, senza dover necessariamente avviare una procedura di assistenza giudiziaria. [267]

In caso di controversia, le autorità preposte al perseguimento penale dovrebbero intervenire conformemente alle disposizioni in materia di assistenza giudiziaria internazionale, il che potrebbe rallentare considerevolmente la procedura penale. Visto l'elevato numero di casi transfrontalieri, la cooperazione internazionale tra le autorità istruttorie rappresenta spesso l'unica alternativa. [268] In presenza di un procedimento penale avviato all'estero contro una condotta punibile anche in quel Paese (ad es. hacking o furto di dati), sarà più facile lo scambio di informazioni tra la Svizzera e quel Paese estero.

Dall'entrata in vigore della Convenzione del Consiglio d'Europa sulla cibercriminalità (Cybercrime Convention, CCC) il 1° gennaio 2012, lo SCOCI ha osservato un aumento significativo dello scambio di informazioni tra gli organismi di polizia criminale. [269] Mediante l'interpol e l'europol, lo SCOCI trasmette alle autorità competenti le segnalazioni relative a contenuti illeciti memorizzati su server esteri, affinché i Paesi interessati cancellino i contenuti secondo le rispettive basi legali e possano avviare un procedimento di perseguimento penale. Sebbene i contenuti vietati secondo il diritto svizzero possano essere accessibili in Svizzera, lo SCOCI non ha un influsso diretto sulla cancellazione o sul blocco di contenuti illeciti all'estero.

5.5.1.2 Limiti delle misure adottate contro trasmissioni televisive estere

Le misure di blocco sono soggette a limiti in materia di diritto internazionale se riguardano trasmissioni televisive. Ai sensi della Convenzione del Consiglio d'Europa sulla televisione transfrontaliera (CETT), vincolante per la Svizzera, l'elaborazione delle misure spetta, in linea di massima, esclusivamente allo Stato emittente.

La diffusione di programmi televisivi veri e propri (vale a dire di contenuti audiovisivi integrali assemblati dall'emittente sotto forma di un programma e trasmessi in tempo reale, il cosiddetto streaming) rappresenta finora un caso raro sulle reti sociali, che propongono piuttosto contributi audiovisivi isolati (video su richiesta e servizi non lineari). In questi casi, il diritto dell'Unione europea prevede l'applicazione del principio dello Stato emittente (o principio del Paese di origine). Per quel che riguarda i ser-

---

[267] Facebook afferma che ogni richiesta proveniente da un'autorità viene esaminata a livello di ammissibilità giuridica e di conformità con le sue condizioni di utilizzo e con le disposizioni legali. Per il primo semestre del 2013, Facebook riferisce che, nel 13 per cento di domande svizzere, ha fornito i dati richiesti su determinati utenti.
https://www.facebook.com/about/government_requests

[268] Hans Bredow-Institut, *Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen an den Jugendmedienschutz*, Entwurf des Endberichts, 2013, punto 2.2.2.2.1, pag. 48.

[269] Rapporto annuale SCOCI 2012, cap. 4, pag. 20.

vizi su richiesta, la relativa direttiva 2010/13/UE concernente i servizi di media audiovisivi non ha carattere vincolante per la Svizzera, ma non si può certo escludere che lo diventerà in futuro.

5.5.2 Applicazione del diritto da parte di privati (ad es. a tutela dei diritti della personalità)

Nel caso di contenuti problematici diffusi su piattaforme sociali, l'applicazione del diritto risulta difficile non solo per le autorità, ma anche per i privati, i cui diritti della personalità potrebbero essere lesi dalla pubblicazione di immagini e testi. [270] La persona che desidera la rimozione di contenuti illeciti pubblicati su una rete sociale da un utente può nella prassi procedere come segue: contatta prima l'autore della violazione e successivamente il gestore della piattaforma, e, infine, se necessario, prende in esame la possibilità di procedere legalmente. Questa procedura si è rivelata efficace in numerosi casi.

5.5.2.1 Diritto applicabile

Per i soggetti privati è importante sapere quale tipo di diritto viene applicato in caso di controversia. Le clausole in materia di diritto applicabile contenute nelle condizioni di utilizzo di piattaforme sociali rimandano solitamente al diritto nazionale o locale del gestore (ad es. diritto dello Stato della California); di norma quest'ultimo non ha sede in Svizzera, pur avendo qui delle filiali. Per quel che concerne il foro giuridico, le condizioni di utilizzo attribuiscono la competenza al tribunale statale che ha sede nel luogo di domicilio del gestore. Occorre tuttavia interrogarsi sulla misura in cui queste clausole sul diritto applicabile e il foro competente possano avere carattere impositivo. Dalle disposizioni imperative del diritto internazionale privato in Svizzera si può evincere quanto segue:

La scelta in materia di diritto applicabile è vincolante solo qualora sia stato stipulato un contratto. A tale scopo è generalmente sufficiente la registrazione di un utente, ma quando la violazione sulla piattaforma riguarda un non utente, il gestore non potrà appellarsi al diritto applicabile enunciato nelle sue condizioni di utilizzo. Se per esempio viene commessa una violazione ai danni della personalità di un individuo, quest'ultimo può intentare un'azione dinnanzi a un tribunale svizzero in conformità alle disposizioni generali concernenti la determinazione del foro competente per pretese derivanti da atti illeciti in controversie internazionali, e richiedere l'applicazione del diritto svizzero in virtù delle disposizioni generali del diritto privato internazionale. Lo stesso dicasi per le violazioni del diritto in materia di concorrenza sleale. In tal caso, per invocare l'applicazione del diritto svizzero è necessario che l'atto sleale produca degli effetti sul mercato svizzero; generalmente è sufficiente che un gestore compia l'atto in questione a detrimento (anche) di utenti svizzeri (art. 136 LDIP [271]). Un gestore estero di una piattaforma di media sociali destinata anche a utenti svizzeri dovrà pertanto attenersi alle disposizioni sancite nella legge federale contro la concorrenza sleale (incluso l'art. 8 LCSl, che disciplina il contenuto lecito delle condizioni generali di contratto), indipendentemente da ciò che prevedono le sue condizioni di utilizzo. Questo principio si applica inoltre alla protezione dei dati: anche gli utenti registrati possono, se lo desiderano, rivolgersi a un tribunale svizzero per risolvere controversie vertenti su violazioni della protezione dei dati secondo le disposizioni di cui alla LPD, a prescindere dalle condizioni di utilizzo e dal diritto applicabile in esse indicato (art. 139 LDIP).

Inoltre, le clausole concernenti il foro giuridico competente e il diritto applicabile contenute nelle condizioni di utilizzo non hanno alcuna validità nel momento in cui il diritto privato internazionale, o eventuali contratti internazionali, stabiliscono, in misura interamente o parzialmente vincolante, il foro giuridico e le condizioni contrattuali vigenti tra l'utente e il gestore. Gli utenti sono altresì tutelati quando stipulano un contratto dalla Svizzera per mezzo di un sito Internet, anche se il gestore ha sede all'estero. In quest'ultimo caso, l'utente con domicilio in Svizzera può far valere le sue pretese nei confronti del

---

[270] Le delucidazioni di cui al punto 5.5.2 si basano su un testo redatto nel febbraio 2013 su mandato dell'Ufficio federale delle comunicazioni da David Rosenthal, docente di diritto dell'informazione e delle telecomunicazioni all'università di Basilea. La versione integrale del testo è disponibile sul sito: http://www.infosociety.admin.ch.

[271] Legge federale del 18 dicembre 1987 sul diritto internazionale privato (LDIP), RS **291**.

gestore dinnanzi a un tribunale svizzero (art. 15 par. 1 lett. c Convenzione di Lugano[272]; art. 114 cpv. 1 lett. a LDIP), che applicherà il diritto (contrattuale) svizzero (art. 120 LDIP).

5.5.2.2 Riconoscimento e soddisfazione delle pretese

L'applicabilità del diritto svizzero e la competenza dei tribunali svizzeri nell'ambito delle condizioni di utilizzo non riescono da sole a garantire che le pretese avanzate nei confronti di gestori stranieri di reti sociali (per lo più americani) acquisiscano effettivamente forza esecutiva. A tale scopo, la persona lesa deve avviare un procedimento di riconoscimento e di esecuzione dinnanzi al tribunale del Paese di domicilio del gestore. Anche nel caso in cui il riconoscimento e l'esecuzione di una sentenza emessa da un tribunale svizzero possano aver luogo in un Paese estero e siano in parte favoriti da accordi internazionali[273], una tale procedura concede spesso (e di nuovo) al gestore la possibilità di opporsi alla competenza del tribunale svizzero (che ha generalmente emesso una decisione in deroga alla clausola sul foro giuridico stabilita nelle condizioni di utilizzo), il che può ostacolare, o perlomeno rallentare, il procedimento di riconoscimento ed esecuzione. Il ventaglio di possibilità a disposizione del gestore dipende, a seconda delle circostanze, anche dal diritto estero applicabile. In tale contesto, alla parte lesa converrebbe far valere eventuali pretese direttamente nel Paese estero in cui si è esplicato l'atto, rinunciando all'applicazione del diritto svizzero.

In entrambi i casi, i costi risultanti dall'avvio di un procedimento giuridico hanno potere dissuasivo. Nel complesso, le controversie vertenti sulle condizioni di utilizzo delle piattaforme sociali costituiscono in Svizzera un'eccezione.

Esistono anche piattaforme sociali estere che accettano ed eseguono "volontariamente" le decisioni pronunciate in Svizzera, anche senza l'avvio di un procedimento di esecuzione all'estero. Le condizioni di utilizzo della maggior parte dei gestori non vietano solo i contenuti "illeciti" (che naturalmente comprendono anche contenuti contrari alla LPD), bensì anche informazioni diffamatorie contro altri utenti o terzi, prescrivendo quindi misure più severe di quelle previste per legge (si veda punto 4.2.2 di cui sopra). I gestori più grandi dispongono di un servizio reclami, visto il numero elevato che ne ricevono giornalmente.

Molti gestori non desiderano effettuare loro stessi alcun apprezzamento giuridico, ma richiedono all'autorità competente del Paese in questione di emettere una decisione esecutiva. Se presentata al gestore, quest'ultimo è tenuto a bloccare i contenuti ritenuti illeciti, anche se la decisione non lo chiama direttamente in causa (ossia, senza che sia convenuto) o che a un tale scopo occorra adire le vie legali. In un caso simile, la persona lesa deve procedere giuridicamente, ma riesce tuttavia a contenere il dispendio di risorse, dal momento che è sufficiente avviare una procedura in Svizzera. Anche in questo caso esistono diverse modalità di procedere, che dipendono principalmente da due aspetti: si tratta innanzitutto di una condotta penalmente rilevante (una mera violazione della sfera privata può costituire l'oggetto di un atto illecito, ma non per questo rientra generalmente nel campo di applicazione del diritto penale, dunque non è punibile, e può essere perseguita "solo" per mezzo di un'azione civile). Secondariamente, l'identità dell'autore della violazione è conosciuta con certezza.

Se si è in presenza di una violazione della personalità ad opera di ignoti, la Svizzera non prevede la possibilità di avviare contro questi ultimi un procedimento giuridico dinnanzi a un tribunale civile. In questi casi occorre agire formalmente contro il gestore della piattaforma, fermo restando che la violazione della personalità non coinvolga nessun'altra persona (ad es. il responsabile del sito sul quale figura un'affermazione lesiva della personalità) e il gestore non sia disposto a rivelare l'identità della persona responsabile. Il diritto svizzero in materia di protezione della personalità offre quindi la possibilità di procedere civilmente contro tutti coloro che "partecipano" a un atto di violazione della persona-

---

[272] Convenzione del 30 ottobre 2007 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (CLug), RS **0.275.12**.

[273] Ad es. nei confronti degli Stati dell'UE e dell'AELS vige la suddetta Convenzione di Lugano concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale.

lità. Secondo la dottrina dominante, i gestori di piattaforme sociali (ad. es. di un blog) appartengono a questa categoria, pur svolgendo un ruolo secondario. [274] Diversamente dalla situazione in cui il gestore è disposto a collaborare, sebbene esiga di prendere visione di una sentenza o di una decisione dell'autorità prima di bloccare un contenuto, un'azione contro un gestore renitente si rivela nella prassi una soluzione realmente efficace solo quando il medesimo è domiciliato in Svizzera o in un Paese in cui è possibile, in modo semplice e rapido, ottenere il riconoscimento e l'esecuzione di una sentenza emessa in Svizzera.

La persona lesa può anche avviare un'azione legale all'estero nel luogo di domicilio del gestore. Questa procedura non comporta necessariamente costi più elevati rispetto a una avviata dinnanzi a un tribunale svizzero, ma non è generalmente possibile senza il ricorso all'assistenza legale e pertanto senza che ne risultino dei costi.

5.5.2.3 Protezione giuridica a scopo precauzionale

A tutela dei diritti della personalità, il diritto vigente prevede la possibilità di presentare domanda di cancellazione, cessazione, accertamento, riparazione morale e risarcimento danni. Considerato il rischio di una diffusione rapida di contenuti diffamatori, s'impone la necessità di garantire quanto prima possibile una protezione a livello giuridico. Nella prassi, la pronuncia giudiziale di misure precauzionali è frequente e consente di impedire che un contenuto lesivo rimanga in rete nel corso di un procedimento giuridico che coinvolge tutte le istanze e potrebbe quindi protrarsi per diversi anni. Per questa ragione, all'inizio del procedimento, o addirittura nella fase ad esso antecedente, viene richiesta la cancellazione temporanea del contenuto in questione o viene emesso un divieto di pubblicazione a titolo provvisorio. In caso di provvedimenti emanati a titolo provvisorio, questa procedura si applica senza indugio e in virtù unicamente delle considerazioni presentate dalla parte attrice, senza ascoltare le altre parti coinvolte o eventuali terzi. Nel caso, invece, di altri provvedimenti precauzionali si procede all'audizione delle parti, che potrebbe protrarsi per qualche settimana.

Nel caso di una misura precauzionale, si opta per una procedura semplificata se la causa è urgente e ha buone possibilità di vittoria (vale a dire se un determinato contenuto è effettivamente illecito), se la scelta di ordinare una misura precauzionale sia sensata in rapporto alle conseguenze comportate alla parte convenuta per la durata del procedimento (ad es. svantaggi conseguenti a misure provvisorie di cancellazione o blocco), o se potrebbe risultare per la parte attrice un danno difficile da riparare (ad es. pecuniariamente). Se viene ordinata una misura precauzionale, l'attore deve avviare un'azione legale contro il convenuto entro i termini prestabiliti, a pena di annullamento della misura.

A livello internazionale, l'applicazione di provvedimenti precauzionali risulta complicata ed è spesso possibile solamente ad azione ritardata. Le decisioni provvisorie ad esempio non rientrano nel campo di applicazione della Convenzione di Lugano,[275] e non possono quindi trarre beneficio della possibilità di una procedura semplificata di riconoscimento ed esecuzione prevista dalla Convenzione. La fase che intercorre tra l'emissione del provvedimento precauzionale e la sua applicazione all'estero può durare diversi mesi.[276]

5.5.2.4 Altri aspetti relativi a una protezione efficace degli interessi privati

Nella prassi, gli strumenti giuridici non riescono a garantire da soli una protezione efficace degli interessi privati. Anche quando un contenuto è stato rimosso da una piattaforma, potrebbe essere infatti

---

[274] Si veda ad es. TF 5A_792/2011 del 14.1.2013 consid. 6.2 (blog della piattaforma del Tribune de Genève); parere di Fanti Sébastien, Remarques, in: *medialex* 2013, pag. 80.

[275] Sentenza CGUE del 21.5.1980 Denilauler / Couchet, Rs. C-125/79: provvedimenti precauzionali che possono essere eseguiti senza che la parte contro cui essi si rivolgono sia stata citata a comparire e senza essere stati prima comunicati a detta parte, non fruiscono del regime di riconoscimento e di esecuzione ivi contemplato.

[276] Per un esempio illustrativo si veda Schneider-Marfels Karl-Jascha, «Facebook, Twitter & Co: "Imperium in imperio"», in: *Jusletter* del 20 febbraio 2012.

necessario ripulire il motore di ricerca da tutte le possibili attestazioni attinenti (se non bloccata dal gestore, la pagina è potenzialmente accessibile nella memoria cache). È consigliato utilizzare una funzione specifica, spesso offerta dai motori di ricerca stessi, che permette di ordinare al crowler di scannerizzare nuovamente una data pagina e, se necessario, di rimuoverla dall'indice di ricerca (a tale scopo occorre inserire l'indirizzo Internet della pagina in questione).

Un altro problema è rappresentato dal fatto che i contenuti (ad es. video), una volta pubblicati, possono essere utilizzati e diffusi da altri utenti (effetto virale). Questo impedisce alla persona lesa di ottenere la cancellazione di una pubblicazione non gradita, nonostante i diritti e gli strumenti giuridici esistenti. In alcuni casi conviene che la persona lesa agisca in modo attivo per difendere la propria reputazione. Un simile comportamento potrebbe sollecitare il gestore della piattaforma a intervenire in modo deciso contro contenuti di natura illecita. In sostanza, i gestori non hanno alcun interesse ad avere una cattiva reputazione o a suscitare la collera degli utenti, non vogliono avere la fama di piattaforme di mobbing su Internet o di diffamazione. L'esperienza mostra che, in caso di pressione pubblica, rimuoveranno rapidamente, o più rapidamente, i rispettivi contenuti, allo scopo di proteggere la propria reputazione, mentre un caso che non attira l'attenzione del pubblico sarà trattato probabilmente con meno celerità. Inversamente, l'attenzione del pubblico accresce anche la pressione sulla vittima e può contribuire a una diffusione incontrollata del contenuto.

6 Questioni giuridiche non approfondite nel rapporto

Oltre alle questioni descritte nei capitoli 4 e 5, i media sociali sollevano una serie di aspetti problematici su vari livelli. Il presente capitolo si limiterà a enunciarli in forma sintetica.

6.1 Applicazione del diritto d'autore nell'ambito dei media sociali

In quest'epoca all'insegna del digitale, le difficoltà riscontrate talvolta nell'applicazione del diritto d'autore e dei diritti di protezione a questo connessi riguardano anche le piattaforme dei media sociali. Il gruppo di lavoro GLDA12, istituito dal DFGP, sta attualmente esaminando provvedimenti volti a contrastare le violazioni del diritto d'autore commesse su Internet (derivanti ad es. dallo scambio di file musicali, video o testuali ottenuti senza licenza mediante la condivisione di file e lo streaming). Nel quadro delle sedute svoltesi sinora, i membri del GLDA12 riconoscono l'esigenza di combattere in modo efficace i modelli commerciali fondati sulla violazione dei diritti d'autore e concordano nel chiedere che i gestori di infrastrutture che ricorrono a modelli commerciali di questo tipo forniscano assistenza nei limiti di quanto ragionevole, delle possibilità tecniche e legali.[277]

Inoltre, dal 2012 la SECO organizza una tavola rotonda allo scopo di esaminare, nel quadro della legislazione vigente, come le violazioni del diritto d'autore su Internet possano essere identificate conformemente alla legge sulla protezione dei dati e perseguite a livello penale.

6.2 Concorrenza tra i media sociali

Il rapporto affronta i singoli aspetti legati alla posizione dominante di determinate piattaforme di media sociali e il loro impatto sugli interessi dell'utenza (effetto di lock in, diritto di accedere alle piattaforme di media sociali [dominanti sul mercato]).

Inoltre l'abuso di una posizione dominante sul mercato in altri settori può essere fronteggiato, anche nel caso dei media sociali, ricorrendo agli usuali strumenti previsti dalle disposizioni generali in materia di concorrenza (segnatamente la legge sui cartelli).

[277] Maggiori informazioni consultabili all'indirizzo: https://www.ige.ch/it/diritti-dautore/glda12.html.

6.3 Offerte delle emittenti radiotelevisive nell'ambito dei media sociali

Come altre imprese mediatiche, anche le emittenti di programmi radiotelevisivi sono sempre più presenti nei media sociali, un ambito nel quale la legge non impone loro particolari limitazioni. Nel quadro della LRTV si è pertanto rinunciato intenzionalmente all'introduzione di un disciplinamento in materia.

La SSR costituisce tuttavia un'eccezione. La sua presenza nei media sociali, finanziata dai proventi del canone radiotelevisivo, rientra nell'ulteriore offerta editoriale, il cui volume deve essere definito nella concessione secondo l'articolo 25 capoverso 3 lettera a della LRTV. Il Consiglio federale propone di disciplinare nel dettaglio le responsabilità derivanti da affermazioni problematiche e di chiarire le competenze in materia di vigilanza. Occorre quindi sancire a livello legislativo che i contributi redatti dalla SSR, e non quelli creati dagli utenti (user generated content), debbano soddisfare determinati requisiti minimi (rispetto della dignità dell'uomo e dei diritti fondamentali, il divieto di rappresentazioni di atti di cruda violenza, protezione dei giovani, in alcuni casi anche il principio dell'oggettività e il principio della pluralità). I requisiti minimi devono valere anche per i contributi redazionali pubblicati in un blog o un forum.[278]

6.4 Comunicazione tra criminali su reti a circuito chiuso

Il presente rapporto pone l'accento sulle reti sociali, che si distinguono per la loro permeabilità e carattere pubblico, nonché sui problemi che ne derivano. La comunicazione segreta concepita per scopi illeciti, come ad esempio lo scambio di materiale pornografico nelle reti P2P, pongono problemi specifici.[279]

Il diritto vigente riconosce in taluni casi la possibilità di contrastare questi atti mediante delle indagini sotto copertura. In virtù dell'ordinanza del Cantone di Svitto sulla polizia, i collaboratori dello SCOCI possono svolgere indagini preliminari sotto copertura nei confronti di pedocriminali in chatroom, su siti Internet o in reti private di condivisione di dati P2P[280]. Inoltre, lo SCOCI effettua per esempio un monitoraggio delle reti P2P alla scopo di individuare qualsiasi reato di natura pedopornografica.[281]

6.5 Spionaggio informatico (monitoraggio da parte di servizi segreti esteri o di privati)

A seguito delle rivelazioni nel 2013 di Edward Snowden (ex collaboratore dei servizi segreti statunitensi, la National Security Agency, NSA), la popolazione ha preso maggiore consapevolezza dell'azione di sorveglianza sulle comunicazioni su Internet esercitata da servizi segreti. [282] Attraverso delle interfacce la NSA riesce a monitorare, raccogliere e conservare informazioni contenute anche sulle piattaforme dei media sociali.

Il fenomeno dello spionaggio informatico, sia che sia effettuato da servizi segreti esteri o da privati, non interessa prevalentemente le piattaforme sociali, ma riguarda sempre più la comunicazione su Internet di natura esclusivamente privata. Nella sua risposta all'interpellanza 13.3558 Eichenberger «Spionaggio informatico. Valutazione e strategia»[283] del 20 giugno 2013, il Consiglio federale rimanda alla «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)» del 27 giugno 2012 e al relativo piano di attuazione, adottato il 15 maggio 2013[284] e concernente le 16 misure previ-

---

[278] Messaggio concernente la modifica della legge federale sulla radiotelevisione (LRTV) del 29 maggio 2013, FF **2013** 4281.

[279] Grazie alla costante attività di monitoraggio, nel 2012 lo SCOCI è riuscito a identificare complessivamente 417 soggetti coinvolti nello scambio di materiale pedopornografico, si veda il rapporto annuale SCOCI 2012, pag. 1.

[280] Rapporto annuale SCOCI 2012, pag. 13.

[281] Si veda ad es. Lentjes Meili Christiane*, Präventiv oder Repressiv? Das Verwirrspiel um verdeckte polizeiliche Operationen, in Festschrift* Donatsch, Zurigo 2012, pag. 437 segg.

[282] Da almeno il 2007, gli Stati Uniti hanno monitorato in modo esteso le telecomunicazioni, in particolare i contenuti Internet, a livello globale e a prescindere dalla presenza di sospetti, e memorizzato i dati ottenuti a titolo preventivo.

[283] http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20133558

[284] http://www.isb.admin.ch/themen/01709/01711/index.html?lang=it

ste dalla Strategia. Grazie a quest'ultima, il Consiglio federale persegue i seguenti obiettivi: individuare precocemente le minacce nello spazio informatico, incrementare la resistenza delle infrastrutture critiche agli attacchi, ridurre i rischi informatici e contrastare gli eventi concreti.

Nella risposta all'interpellanza 13.3033 Schwaab «Come proteggere i dati personali di cittadini svizzeri in possesso di imprese americane?»[285] del 6 marzo 2013, il Consiglio federale si è espresso su svariate questioni legate al quadro legislativo svizzero e sulla prassi riguardante la richiesta da parte delle autorità statunitensi dei dati personali di cittadini di Paesi terzi salvati nella nuvola informatica. Oltre alla responsabilità individuale di ogni singolo individuo nell'ambito della gestione dei propri dati, il Consiglio federale richiama l'attenzione sul programma di sensibilizzazione «Giovani e media» della Confederazione[286] e sulla funzione consultiva dell'IFPDT. Fornisce inoltre delucidazioni sul diritto contrattuale e sulle possibilità di applicazione della LDIP[287] e della LugÜ[288] e rimanda agli attuali lavori di revisione della LPD[289], nell'ambito della quale occorrerà verificare se le disposizioni legali vigenti sono realmente sufficienti.

[285] http://www.parlament.ch/i/suche/pagine/geschaefte.aspx?gesch_id=20133033

[286] http://www.bsv.admin.ch/themen/kinder_jugend_alter/00071/03045/

[287] Legge federale del 18 dicembre 1987 sul diritto internazionale privato (LDIP), RS **291**.

[288] RS **0.275.12**.

[289] RS **235.1**.

7 Raccomandazioni

Qui di seguito sono illustrate le azioni raccomandate per far fronte ai problemi descritti nei capitoli 4 e 5. Come esposto, il diritto materiale svizzero è spesso sufficiente. Tuttavia, nella pratica molti problemi non possono essere risolti unicamente, o forse principalmente, mediante il ricorso a strumenti giuridici. In questa sede saranno pertanto affrontati, oltre agli aspetti legali, anche questioni relative per esempio all'informazione e alla sensibilizzazione.

7.1 Necessità di introdurre nuove prescrizioni legali

7.1.1 Situazione iniziale: rischio di un disciplinamento eccessivo

Come precedentemente esposto, è un fatto possibile, ma comunque non certo, che le prescrizioni legali in vigore e la loro applicazione (legale) non offrano in casi particolari risposte soddisfacenti ai problemi sollevati dai media sociali. Non si esclude tuttavia la necessità di introdurre misure disciplinari puntuali, impedendo tuttavia l'attivismo da parte dei legislatori oppure l'introduzione di un disciplinamento eccessivo. Come avviene in altri settori soggetti a rapidi cambiamenti, azioni avventate (ad es. l'emanazione di prescrizioni a titolo precauzionale) rischiano di produrre conseguenze inattese.

In ogni caso specifico, occorre verificare con esattezza se i meccanismi di autoregolamentazione esistenti non siano sufficienti (ad es. il codice di condotta di cui al punto 5.4.1 summenzionato relativo al fornitore svizzero di servizi di hosting membro dell'associazione Simsa, come pure le condizioni di utilizzo di alcune piattaforme estere, come Facebook o Twitter).

7.1.2 Potere legislativo del singolo Stato limitato dal contesto internazionale

L'azione del legislatore svizzero è ostacolata da un contesto fortemente transfrontaliero. Molti problemi non possono essere risolti in modo efficace attraverso disposizioni legali emesse in modo isolato da questo o quell'altro Paese. Come menzionato, molte delle piattaforme largamente utilizzate in Svizzera hanno la propria sede all'estero.

Al posto di interventi di regolamentazione intrapresi da singoli Stati, che comportano un dispendio notevole di risorse e sono efficaci soltanto in misura limitata, occorre rafforzare gli sforzi profusi a livello internazionale: il Consiglio d'Europa fa giustamente notare che le misure di disciplinamento previste da un ordinamento giuridico potrebbero pregiudicare notevolmente l'accesso e l'utilizzazione Internet in altri ordinamenti giuridici, nonché la funzionalità dell'infrastruttura Internet[290]. Pertanto lo scambio di informazioni transfrontaliero in Internet necessita di confronti multilaterali, soprattutto per quel che concerne le fattispecie contemplate da diversi ordinamenti giuridici, un caso che si verifica sempre più di frequente nell'ambito di sviluppo di piattaforme transfrontaliere, come per esempio le reti sociali, oppure con l'avvento del *cloud computing* (nuvola informatica)[291].

7.1.3 Rispetto della coerenza dell'intero ordinamento giuridico

Qualora si riscontri la necessità di disciplinare a livello nazionale alcuni ambiti, occorre prestare particolare attenzione affinché la coerenza dell'intero ordinamento giuridico sia preservata. Molti aspetti problematici in relazione ai media sociali si presentano anche in altri ambiti di vita: il diritto all'oblio e il mancato controllo sui propri dati riguarda inoltre altre forme di comunicazione online e più in generale il nostro quotidiano[292]; la protezione della personalità è minacciata anche da affermazioni divulgate dai tradizionali mass media (stampa e radiodiffusione); la protezione della gioventù è messa in pericolo dai giochi per computer; la pornografia non si limita a Internet ecc.

---

[290] Si veda ad es. la spiegazione dei principi che reggono la governance di Internet e la raccomandazione CM/Rec(2011)8 sulla protezione e promozione dell'universalità, integrità ed apertura di Internet.

[291] Per l'approfondimento di questi aspetti, il gruppo Ad Hoc Advisory Group on Cross-Border Internet, istituito dal Consiglio d'Europa, raccomanda l'approccio *multi-stakeholder participation* adottato dal Consiglio d'Europa per questioni simili.

[292] Si veda ad es. Flückiger Alexandre, *L'autodétermination en matière de données personnelles :un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?,* in: AJP/PJA 2013, pag. 837 segg.

Molteplici questioni sono disciplinate da norme generali, non specifiche ai media sociali, come quelle contenute nel Codice penale, nel Codice civile o nella legge federale sulla protezione dei dati. L'introduzione di disposizioni isolate concernenti specificatamente il fenomeno delle reti sociali potrebbe comportare una frammentazione e rischiare di compromettere la coerenza dell'ordinamento giuridico. In linea generale si raccomanda pertanto di sviluppare ulteriormente il quadro legislativo esistente e di chiedersi se l'evoluzione di un dato problema concerni unicamente le reti sociali, o anche altri ambiti di vita.

7.2 Al vaglio una legge specifica per le reti sociali

7.2.1 Situazione iniziale

Nel postulato 11.3912 «Diamo un quadro legale ai social media» ci si interroga se sia possibile, come lo è stato per l'ambito radiotelevisivo, elaborare un disciplinamento specifico per rispondere all'evoluzione dei media sociali.

7.2.2 Competenza legislativa della Confederazione

Occorre in primo luogo verificare se la Confederazione sia competente per l'elaborazione di disposizioni disciplinanti il contenuto dei media sociali. Per quel che concerne la comunicazione pubblica su piattaforme di media sociali, la Confederazione può rifarsi all'articolo 93 capoverso 1 della Costituzione, che le conferisce la competenza di legiferare su forme di diffusione pubblica di produzioni e informazioni tramite tecniche di telecomunicazione. La Confederazione ha pertanto facoltà di legiferare in merito ai contenuti diffusi dai media sociali. A questi ultimi i mandati di prestazione non sono attribuiti direttamente da norme costituzionali, come è il caso della radio e della televisione (art. 93 cpv. 2 Cost.). La Confederazione può tuttavia decidere liberamente di emanare in via legislativa direttive sul contenuto di altre forme di diffusione pubblica di produzioni e informazioni tramite tecniche di telecomunicazione[293]. Così facendo, la Confederazione può adempiere il suo obbligo fondamentale di tutelare uno scambio libero ed equo di informazioni e opinioni.

Nel caso di contenuti scambiati sulle reti sociali non destinati al pubblico, la Confederazione non può far valere l'articolo 93 della Costituzione. Ciò nonostante, la competenza legislativa può essere fatta derivare da diverse disposizioni costituzionali. Per esempio l'articolo 92 capoverso 1 della Costituzione definisce le telecomunicazioni quale competenza della Confederazione. In virtù di questo, la LTC non disciplina unicamente la trasmissione tramite telecomunicazione, ma anche lo spamming o i servizi a valore aggiunto.[294] Il legislatore può inoltre applicare in materia civile e penale rispettivamente l'articolo 122 e l'articolo 123 della Costituzione. In questo ambito esso sarebbe inoltre competente, se il caso lo richiede, per l'emanazione di eventuali disposizioni specifiche ai media sociali.

7.2.3 Necessità di un disciplinamento specifico?

Un disciplinamento specifico per le affermazioni pubbliche sui media sociali, simile a quello vigente in materia di radiodiffusione, è giustificato soltanto nel caso in cui serva a mantenere o promuovere la libertà nella comunicazione pubblica. Vista l'offerta variegata delle diverse piattaforme sociali, questa ipotesi pare essere meno probabile che nel campo della radiotelevisione, caratterizzato usualmente dalla carenza dell'offerta (carenza di frequenze). Anche in questo contesto, la necessità di mandati di prestazione è meno marcata in presenza di diversi canali di diffusione rispetto a una situazione di monopolio o a un'emittente di programmi (pubblici) che occupa una posizione dominante sul mercato.

Sembrerebbe quindi opportuno legiferare solo nel caso in cui le azioni intraprese non siano sufficienti a garantire la libera comunicazione, indispensabile dal un punto di vista democratico e per lo sviluppo del singolo. Questo potrebbe verificarsi quando la pluralità dei media, imprescindibile dai processi

---

[293] BU 1983 N 1353 (voto del consigliere nazionale Schüle).

[294] Messaggio relativo alla modifica della legge sulle telecomunicazioni (LTC) del 12 novembre 2003, FF **2003** 6898, 6934.

sociali e democratici, non trova più espressione, poiché per esempio alcune comunità minoritarie non hanno opportunità reali di fare ascoltare la propria voce in modo efficace.

Nell'ambito delle reti sociali non è tuttavia possibile escludere che alcune piattaforme acquisiscano un'importanza preponderante, che non viene regolata a sufficienza dalle forze in gioco nel libero mercato. Un intervento statale consentirebbe di garantire la pluralità di opinioni, indispensabile sotto il profilo sociale e democratico. Questo sarebbe il caso in cui determinati gruppi della popolazione non hanno possibilità reali di partecipare alla comunicazione sulle principali piattaforme di media sociali; al momento non esistono segnali a favore di quest'ipotesi. Al contrario, si può supporre che attualmente anche le minoranze possano ricevere maggior ascolto grazie alle piattaforme. A prescindere da questo, la maggior parte dei più importanti fornitori ha sede all'estero e i mandati di prestazione del legislatore svizzero non avrebbero alcun influsso significativo. Nell'ottica attuale, non si intravede la necessità di emanare una disposizione specifica in materia di media sociali.

7.2.4 Necessità di adeguare la legislazione vigente?

Come precedentemente esposto, un'eventuale risposta ai nuovi problemi sollevati dai media sociali non risiede in una legge specifica o in disposizioni isolate per i media sociali, bensì in un adeguamento delle attuali prescrizioni legali, spesso formulate in termini generali. Se queste dovessero risultare puntualmente inefficienti, si dovrà esaminare la possibilità di completare la legislazione vigente.

7.2.4.1 Esame approfondito degli aspetti legali concernenti la protezione dei dati

Nel capitolo 4 sono stati individuati numerosi problemi che i media sociali pongono in relazione alle disposizioni legislative in materia di protezione dei dati. Questo discorso vale ad esempio per il diritto all'oblio o, in generale, per la mancanza di controllo degli utenti sui propri dati.

Quale legge quadro, la legge federale sulla protezione dei dati (LPD) vigente in Svizzera è formulata in termini molto generali. Applicata con giudizio, la LPD consente generalmente alle autorità e ai tribunali competenti di tener in considerazione i nuovi problemi legati alla protezione dei dati. Occorre approfondire ulteriormente se ciò sia applicabile senza eccezioni o se occorra adeguare la legislazione in vigore, tenendo altresì conto delle revisioni attualmente in corso delle disposizioni in materia di protezione dei dati dell'Unione europea e del Consiglio d'Europa. I relativi lavori di verifica sono attualmente condotti sotto l'egida del DFGP. Un gruppo di accompagnamento in materia di protezione dei dati (LPD), ampiamente rappresentato, si sta occupando di analizzare l'intera legge sulla protezione dei dati e le relative misure di applicazione. L'analisi comprende le questioni sollevate da nuovi fenomeni, come quello dei media sociali.

Il DFGP è incaricato di sottoporre al Consiglio federale, entro il 2014, delle proposte sulla seguente modalità di procedere.

7.2.4.2 Al vaglio un eventuale disciplinamento in materia di responsabilità

Come illustrato precedentemente (punto 5.3), a fronte degli attuali sviluppi e dei segnali della giustizia nel campo del diritto civile, è opportuno che il Consiglio federale riesamini la necessità di un intervento legislativo in materia di responsabilità dei fornitori di servizi Internet (vale a dire dei fornitori di servizi di accesso e di hosting, come anche dei gestori di piattaforme). Un esame simile rappresenta un compito delicato, considerato il fatto che nel frattempo anche all'estero si è sviluppata una giurisprudenza differente, che dovrà essere analizzata scrupolosamente. Dei lavori in tal senso saranno avviati nel corso del 2013, sotto l'egida del DFGP.

Nel quadro di questa fase non si esclude la possibilità di esaminare ulteriori aspetti problematici, come per esempio l'adeguamento delle disposizioni vigenti in materia di cancellazione e di blocco dell'accesso a contenuti illeciti.

7.2.4.3 Legislazione in materia di telecomunicazioni e piattaforme dei media sociali

Una classificazione giuridica dei diversi servizi di trasmissione, offerti in parte anche dai media sociali, risulta un'operazione complessa. La legislazione vigente in materia di telecomunicazioni, elaborata in un'epoca in cui non esistevano ancora i servizi indipendenti dall'infrastruttura di trasporto, non è in grado di offrire risposte adeguate. Oggigiorno sono adottati altri modelli commerciali (ad es. il finanziamento attraverso la pubblicità), vigono diverse condizioni tecniche ed esistono diversi tipi di servizi di trasporto, che possono essere offerti in tutto il mondo investendo poche risorse. Le disposizioni legislative in materia di telecomunicazioni applicabili a questo tipo di servizi dovrebbero essere esaminate non solo in relazione ai media sociali, ma anche a tutti quei servizi che (spesso gratuitamente) sono forniti per esempio su Internet, senza che sia necessario richiedere l'autorizzazione al proprio fornitore Internet (i cosiddetti servizi *over the top*). Questi aspetti saranno approfonditi nel quadro del progetto di consultazione concernente la revisione della legge sulle telecomunicazioni, che il Consiglio federale intende commissionare nel periodo legislativo ancora in corso.

7.2.4.4 Esame di un disciplinamento in materia di portabilità dei dati

Occorre osservare se i media sociali intendano mantenere i propri utenti impedendo il trasferimento dei loro dati a piattaforme concorrenti (si veda il punto 4.3.7 di cui sopra). La Confederazione dovrebbe seguire da vicino questo mercato e, all'occorrenza, introdurre un diritto alla portabilità dei dati. Eventualmente, potrebbe rivelarsi opportuno disciplinare le interfacce tra le diverse piattaforme di media sociali, prescrivendo ad esempio a quelle più importanti di consentire ai loro utenti di scambiare dati, sotto forma ad esempio di messaggi privati, anche su altre piattaforme. Nei prossimi anni, sarà forse possibile trarre vantaggio dalle esperienze realizzate all'estero e basarsi anche su quest'ultime per decidere in merito alla necessità di legiferare.

7.3 Informazione e sensibilizzazione

A livello sia nazionale che internazionale, si è consapevoli del fatto che le opportunità e i rischi legati alle reti sociali non possano essere influenzati solamente dalle prescrizioni legali (e dalla loro applicazione), e che sia possibile giungere a dei risultati soddisfacenti solo attraverso il ricorso a strumenti stragiudiziali, come la promozione della consapevolezza nelle cerchie interessate.

7.3.1 Diritto all'oblio

L'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) richiama l'attenzione sul fatto che oggigiorno le soluzioni tecniche esistenti non proteggono sufficientemente i dati pubblicati da qualsiasi copia non autorizzata da parte di terzi e da un'eventuale ridiffusione dopo la loro cancellazione "ufficiale"[295]. Al contempo si constata che soluzioni puramente tecniche non sono sufficienti per applicare il diritto all'oblio in un sistema a circuito aperto, come è il caso di Internet. Occorre piuttosto optare per un approccio interdisciplinare, che definisca questo diritto sotto il profilo sia tecnico che giuridico[296].

Il rispetto del diritto all'oblio sulle piattaforme di media sociali può essere tuttavia in molti casi favorito da un comportamento previdente. Come raccomanda per esempio l'IFPDT, prima di pubblicare i propri dati occorre sempre domandarsi se si è disposti a renderne conto in occasione di un colloquio di lavoro, anche a distanza di 10 anni[297]. Non dovrebbero inoltre venire pubblicati dati personali appartenenti a terzi. Questi principi, pur essendo generalmente conosciuti, dovrebbero essere richiamati alla memoria e comprovati da esempi chiari. Un'azione in tal senso può essere intrapresa nel quadro del programma nazionale «Giovani e media».

---

[295] European Network and Information Security Agency (ENISA), The right to be forgotten – between expectations and practice, Heraklion 2011.

[296] ENISA, The right to be forgotten, pag. 11 segg.

[297] http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00693/index.html?lang=it.

7.3.2 Violazioni dell'onore e della personalità, bullismo e stalking su Internet

La divulgazione sulle reti sociali di informazioni false, giudizi lesivi dell'onore e rivelazioni illecite è un aspetto disciplinato a livello penale, civile ed economico nel diritto svizzero (si veda il punto 4.4.1.3 di cui sopra). La modalità attraverso cui un soggetto privato può procedere legalmente contro l'autore di una violazione di un diritto della personalità è descritta al punto 5.5.2. Resta tuttavia il problema che le informazioni diffamatorie possono diffondersi con estrema velocità e su ampia scala.

Per quel che concerne il mobbing e lo stalking su Internet, il Consiglio federale ha ripetutamente constatato che allo stato attuale non esistono argomentazioni che depongono a favore di un'insufficienza degli attuali strumenti giuridici di diritto penale (punto 4.4.2.3 di cui sopra).

Le disposizioni chiare in relazione al diritto materiale vigente in materia di violazioni della personalità nel caso di mobbing e stalking su Internet non presumono tuttavia che gli utenti delle piattaforme di media sociali ne siano a conoscenza. In tal caso potrebbe essere utile elaborare un quadro legislativo facilmente comprensibile, integrandovi eventuali raccomandazioni. In ambito scolastico esistono già iniziative, come educa guides[298] o la piattaforma «Giovani e media»[299], che potrebbero essere ampliate in questo senso. In relazione ad altri gruppi target e condizioni di vita, occorre esaminare quali iniziative e offerte siano più appropriate per l'adempimento di questo compito e come queste possano essere realizzate.

7.3.3 Bambini e giovani

Come menzionato precedentemente (punto 4.6.1.3), il Consiglio federale esaminerà la necessità di rafforzare la protezione dei dati dei minorenni nel quadro della revisione della legge sulla protezione dei dati.[300] Il ricorso a questi strumenti giuridici non rappresenta tuttavia una misura sufficiente a garantire la protezione della gioventù dai rischi dei media. D'importanza centrale è la promozione delle competenze mediali di bambini e adolescenti, nonché delle loro persone di riferimento, in relazione ai vantaggi e svantaggi dei media sociali. In tal contesto s'inserisce il programma nazionale «Gioventù e media»[301], lanciato per il periodo 2011-2015 dal Consiglio federale mediante decisione dell'11 giugno 2010. Questo programma si propone di contribuire affinché i genitori, gli insegnanti e le persone di riferimento dispongano delle competenza mediali necessarie ad accompagnare attivamente le attività mediali di bambini e giovani. Il sito http://www.giovaniemedia.ch/it/home.html, che funge da portale di riferimento per la protezione dei giovani svizzeri dai rischi dei media, offre sistematicamente una panoramica delle offerte informative e didattiche fornite in Svizzera nonché delle strategie e misure adottate a livello cantonale nel campo della protezione dei giovani dai rischi dei media. Nel quadro del programma è stato pubblicato il manuale «Competenze mediali – consigli per un utilizzo sicuro dei media digitali» volto a fornire informazioni pratiche a genitori, bambini e insegnanti[302] su temi quali il mobbing su Internet, le chat, i videogiochi, la pornografia e le reti sociali. Viene inoltre affrontata esplicitamente la questione se sia giusto che gli insegnanti e i genitori stringano amicizia con i giovani sulle reti sociali. Il programma promuove altresì la collaborazione tra diversi enti e gruppi di contatto operanti in questo ambito, e sostiene gli specialisti in campagne di sensibilizzazione. Vengono inoltre promosse la sicurezza qualitativa delle attuali offerte e l'innovazione dei metodi di trasmissione delle competenze mediali (educazione tra pari, strategie di accesso a tutti i gruppi della popolazione).

Competenti in ambito scolastico, i Cantoni ricoprono un ruolo centrale nell'attività di promozione delle competenze TIC. La CDPE attua una strategia tesa all'integrazione delle TIC nei programmi didatti-

---

[298] http://guides.educa.ch/it.

[299] http://www.jugendundmedien.ch/home.html.

[300] Rapporto del Consiglio federale concernente la valutazione della legge federale sulla protezione dei dati del 9.12.2011, punto 5.2.2 (FF **2012** 227).

[301] http://www.giovaniemedia.ch/it/home.html.

[302] http://www.giovaniemedia.ch/fileadmin/user_upload/Chancen_und_Gefahren/guida_FAQ_Medienkompetenz_it.pdf .

ci[303], e formula inoltre raccomandazioni in merito alla formazione degli insegnanti nel campo delle tecnologie dell'informazione e della comunicazione[304] e alla definizione del profilo di corsi supplementari rivolti a coloro che si stanno formando in pedagogia mediatica[305]. Il sito educativo «educa.ch» mette a disposizione degli insegnanti materiali didattici e ulteriori informazioni sul tema, come per esempio l'opuscolo della Prevenzione svizzera della criminalità «Safersurfing - Sicurezza nei Social network» [306], che informa sul mobbing su Internet, sulle molestie sessuali e sull'impiego corretto dei propri dati personali sulle reti sociali. Nel gennaio 2013, questa associazione ha pubblicato anche l'opuscolo «My little Safebook» sull'uso sicuro dei media sociali da parte di genitori e giovani[307].

Oltre alle misure di promozione summenzionate, il Consiglio federale ha incaricato l'Ufficio federale delle assicurazioni sociali (UFAS) di elaborare, nel quadro del programma nazionale «Gioventù e media», delle raccomandazioni su come proteggere in futuro i giovani svizzeri dai rischi dei media.

Per l'adempimento di questo compito, l'UFAS ha istituito un gruppo di esperti costituito da rappresentanti della Confederazione, dei Cantoni e del settore economico e ha conferito quattro mandati di ricerca per l'elaborazione di basi solide:

Mandato 1: esame delle tendenze di sviluppo e di utilizzo nel ramo dei media digitali e delle sfide poste in materia di protezione dei giovani dai rischi dei media (autunno 2012 – estate 2013).

Mandato 2: rilevamento ed esame delle attività di disciplinamento dei Cantoni (primavera 2013 – estate 2014).

Mandato 3: valutazione dell'attuazione e dell'efficacia delle misure di autoregolamentazione dei settori in Svizzera (film, videogiochi, telecomunicazioni e Internet) (primavera 2013 – estate 2014).

Mandato 4: analisi dei modelli di disciplinamento adottati in diversi Paesi concernenti specificamente i media o settori che coinvolgono i media, identificazione di esempi di "buona prassi" e formulazione di raccomandazioni per la Svizzera (primavera 2013 – estate 2014).

Entro il 2015 si dovrà poter stabilire in quale misura sussiste la necessità di legiferare a livello federale e se occorre creare basi costituzionali.

7.3.4 Ampliamento delle competenze mediali della popolazione

Come precedentemente esposto, in ambito scolastico sono già stati operati degli interventi volti a migliorare le competenze mediali dei bambini e dei giovani, come anche delle loro persone di riferimento. Dal momento che i media sociali rappresentano un fenomeno recente e dinamico, i principali siti Internet in materia sono tenuti a verificare costantemente l'attualità delle informazioni pubblicate ed eventualmente modificarle.

Converrebbe inoltre esaminare la misura in cui l'ampliamento delle competenze mediali, in particolare l'utilizzo di media sociali, possa interessare altri gruppi target.[308]Si presenta altresì la possibilità di

---

[303] Strategia della CDPE nel campo delle tecnologie dell'informazione e della comunicazione e dei media del 01.03.2007 (http://edudoc.ch/record/30020/files/ICT_d.pdf?version=1, disponibile solo in tedesco). Vedi anche il documento esplicativo delle tecnologie dell'informazione e della comunicazione nel campo dell'istruzione dell'08.06.2000 (http://www.edudoc.ch/static/web/arbeiten/erkl_ikt_d.pdf, disponibile solo in tedesco).

[304] Empfehlungen für die Grundausbildung und Weiterbildung der Lehrpersonen an der Volksschule und der Sekundarstufe II im Bereich der Informations- und Kommunikationstechnologien vom 25.04.2004; consultabile all'indirizzo: http://www.edudoc.ch/static/web/aktuell/medienmitt/empf_ict_lb_d.pdf

[305] http://edudoc.ch/record/38148/files/Profil_ICT_d.pdf.

[306] http://guides.educa.ch/sites/default/files/sicherheit_netzwerke_i.pdf.

[307] http://news.skppsc.ch/it/.

[308] Si veda per esempio l'opuscolo a fumetti «Storie di Internet…che nessuno vorrebbe vivere» rivolto al grande pubblico, http://www.geschichtenausdeminternet.ch/index_it.html#

impiegare i media sociali per tutti i gruppi target per meglio informare e sensibilizzare in merito a questioni specifiche.

8 Risposta alle domande del postulato

A fronte delle considerazioni precedentemente esposte, è possibile rispondere alle domande sollevate dal postulato come di seguito riportato:

- Come si presenta la legislazione attuale, in Svizzera e all'estero, relativa ai social media?

Per quanto si può constatare, in Svizzera come all'estero esistono finora poche disposizioni che riguardano specificatamente ed esclusivamente il nuovo fenomeno dei media sociali. Sono state piuttosto le prescrizioni legali vigenti ad essere applicate finora anche alla comunicazione sulle reti sociali.

- Cosa pensa il Consiglio federale dell'elaborazione di una legge consacrata ai social media, che consideri le peculiarità di queste nuove piattaforme di comunicazione?

Considerata la situazione attuale, non si riscontra la necessità di elaborare una legge sui media sociali, alla stregua delle disposizioni specifiche in ambito radiotelevisivo.

- Quali aspetti presentano delle lacune? Come possono essere colmate?

L'esperienza acquisita finora non porta a rilevare l'esistenza di lacune gravi nel diritto svizzero vigente. La maggior parte delle disposizioni formulate in modo generale nella legislazione attuale (ad es. LPD, CP, CC, LCSI), se applicate con giudizio, consentono di fornire risposte adeguate a gran parte dei problemi che le piattaforme sociali pongono o potrebbero porre ai singoli o all'intera collettività. Non è tuttavia possibile stabilire con certezza se queste disposizioni saranno efficaci nella pratica. In taluni ambiti si intravede la possibilità di effettuare interventi di miglioramento puntuali. Pertanto si rendono necessari o sono già in corso di elaborazione chiarimenti relativi a diversi aspetti (ad es. protezione dei dati e protezione della gioventù). Occorre sempre tener presente che queste analisi non si limitano al settore dei media sociali, ma interessano anche tante altre questioni.

9 Passi successivi

Come esposto nel capitolo 7, sono attualmente in corso diverse attività in seno all'Amministrazione federale che interessano anche eventuali aspetti giuridici nell'ambito dei media sociali.

- Al momento le questioni relative al diritto in materia di protezione dei dati sono affrontate nel quadro dei lavori di revisione della LPT (svolta sotto l'egida del DFGP). I problemi sollevati dalle piattaforme sociali riguardano soltanto uno dei molteplici ambiti che devono essere esaminati in questo contesto. Il diritto all'oblio e le questioni giuridiche concernenti la mancanza di controllo degli utenti sui propri dati nelle reti sociali (e un certo miglioramento della situazione grazie a impostazioni che favoriscono la protezione dei dati) ricoprono un'importanza centrale. Il DFGP ha ricevuto il mandato di sottoporre al Consiglio federale entro la fine del 2014 delle proposte sui successivi passi da intraprendere.

- Attualmente i problemi legati alla protezione della gioventù saranno analizzati entro il 2015 nel quadro del progetto «Gioventù e media», diretto dall'Ufficio federale delle assicurazioni sociali. Questo progetto mira a chiarire se sussiste la necessità di legiferare a livello federale e se eventualmente sia opportuno introdurre nuove basi per la protezione di bambini e adolescenti. Saranno inoltre formulate raccomandazioni sulla gestione futura della protezione dei giovani dai rischi dei media.

È inoltre opportuno intraprendere altre attività:

- Occorre esaminare la necessità di un intervento legislativo in materia civile allo scopo di disciplinare il riconoscimento della responsabilità sia dei gestori delle piattaforme che dei fornitori di prestazioni tecniche (fornitori di servizi di hostig e di accesso). Questo chiarimento non riguarda solamente le reti sociali, ma anche più in generale la responsabilità giuridica dei fornitori di servizi Internet (*provider*). Il DFGP si confronterà con questa questione e, se è necessaria una modifica di legge, sottoporrà al Consiglio federale un progetto di consultazione.

- In futuro, bisognerà inoltre esaminare quali saranno le regole in materia di diritto delle telecomunicazioni applicabili ai media sociali. Finora sottostanno solo eccezionalmente alle prescrizioni della legge sulle telecomunicazioni (per es. obbligo di notifica, struttura dei prezzi trasparente, lotta contro gli spam). Questi aspetti saranno chiariti dal DATEC nel quadro del progetto di revisione della LTC. Stando alla pianificazione attuale, la revisione della LTC sarà commissionata dal Consiglio federale nel corso della presente legislatura.

- In vista di un eventuale disciplinamento il DATEC si dedicherà anche alla questione che riguarda la possibilità che certi media sociali intendano mantenere i propri clienti impedendo loro di trasferire i propri dati ad imprese concorrenti. In tal caso, potrà in futuro incombere la necessità di introdurre un **diritto di portabilità dei dati** o di disciplinare le interfacce tra le diverse reti sociali. In questo ambito sarà auspicabile ispirarsi agli eventuali lavori legislativi svolti all'estero in tal senso.

Le diverse attività e analisi non concernono esclusivamente i media sociali, ma devono essere considerate in relazione all'intero sistema giuridico. È tuttavia importante che i diversi aspetti costituiscano un quadro generale coerente a livello di contenuto anche per quel che concerne i media sociali. A tale scopo è essenziale che sia garantita la circolazione delle informazioni tra i servizi coinvolti.

Tenendo conto delle numerose attività di disciplinamento note, ed di altre eventuali, che presentano un legame più o meno stretto con i media sociali, è evidente che si corre il rischio di perdere di vista la problematica nel suo insieme. A medio termine, appare opportuno fare nuovamente il punto attuale della situazione in relazione ai media sociali. Questa analisi, che verterà inoltre sui cambiamenti rapidi a livello internazionale e sulla giurisprudenza derivante da numerose controversie, consentirà di mostrare i punti di forza e di debolezza della legislazione in vigore.

Allo stato attuale, sarebbe auspicabile tracciare, in forma di bilancio intermedio, il punto della situazione delle basi legali sui media sociali in vigore da questo momento fino al 2016, anno in cui saranno conclusi i suddetti lavori e sarà meglio definito l'orientamento da seguire.

10 Abbreviazioni, letteratura, referenze

10.1 Elenco delle abbreviazioni

BGBl	Bundesgesetzblatt (Gazzetta ufficiale della Repubblica federale di Germania)
Blog	diario elettronico, diario o giornale su un sito web
Cap.	Capitolo
CC	Codice civile svizzero
CDPE	Conferenza svizzera dei direttori cantonali della pubblica educazione
CEDU	Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali
CESE	Comitato economico e sociale europeo
cfr.	confronta
CGUE	Corte di giustizia dell'Unione europea (autorità giudiziaria suprema dell'Unione europea)
CLug	Convenzione di Lugano
CO	Codice delle obbligazioni
Corte EDU	Corte Europea dei Diritti dell'Uomo
Cost.	Costituzione
CP	Codice penale svizzero
CPM	Codice penale militare
DEFR	Dipartimento federale dell'economia, della formazione e della ricerca
DFGP	Dipartimento federale di giustizia e polizia
DPMin	Legge sul diritto penale minorile
Ed.	Editore
ENISA	European Network and Information Security Agency (Agenzia europea per la sicurezza delle reti e dell'informazione)
FF	Foglio ufficiali
FTC	Federal Trade Commission (autorità federale statunitense garante della concorrenza e della tutela dei consumatori).
GLDA12	Gruppo di lavoro incaricato di ottimizzare la gestione collettiva dei diritti d'autore e di quelli affini
GU	Gazzetta ufficiale dell'Unione europea
H.R.	House of Representatives (Camera dei rappresentanti del Congresso statunitense)
IFPDT	Incaricato federale della protezione dei dati e della trasparenza
LATer	Legge sugli agenti terapeutici
LCart	Legge sui cartelli
LCSI	Legge contro la concorrenza sleale (LCSl)
LDA	Legge sul diritto d'autore
LDIP	Legge sul diritto internazionale privato
LDis	Legge sui disabili
LPAG	Legge sulla promozione delle attività giovanili extrascolastiche
LPD	Legge sulla protezione dei dati
LRTV	Legge sulla radiotelevisione
LTC	Legge sulle telecomunicazioni
n.	numero
ODerr	Ordinanza sulle derrate alimentari e gli oggetti d'uso

ODis	Ordinanza sui disabili
OPAG	Ordinanza sulla promozione delle attività giovanili extrascolastiche
ORTV	Ordinanza sulla radiotelevisione
OTab	Ordinanza sul tabacco
p. es.	per esempio
PPMin	Procedura penale minorile
RSS	Really Simple Syndication, formato che permette di rimanere aggiornati sulle modifiche a siti web
SCOCI	Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet
SECO	Segreteria di Stato dell'economia
SKP	Prevenzione Svizzera della Criminalità
SR	Raccolta sistematica del diritto federale della Svizzera
SSR	Società svizzera di radiotelevisione
TIC	Tecnologie dell'informazione e della comunicazione
U.S.C.	United States Code (raccolta e codifica delle leggi federali degli Stati Uniti)
UE	Unione europea
UFCOM	Ufficio federale delle comunicazioni
UFSP	Ufficio federale della sanità pubblica
WLAN	Wireless Local Area Network

10.2 Letteratura

Aguiton C./Cardon D., «The Strength of Weak Cooperation: an Attempt to Understand the Meaning of Web 2.0», *Communication & Strategies*, n.65, 1^{o} trimestre 2007 (**cit. Aguiton C./Cardon D.**).

Bächli Marc, «Das Recht am eigenen Bild. Die Verwendung von Personenbildern in den Medien, in der Kunst, der Wissenschaft und in der Werbung aus der Sicht der abgebildeten Person», Basilea 2002 (**cit. Bächli Marc, *Das Recht am eigenen Bild*, Basilea 2002**).

Baeriswyl Bruno, «Kleingedrucktes unter der Lupe - Die Allgemeinen Geschäftsbedingungen (AGB) von Sozialen Netzwerken versprechen keinen Datenschutz», in: *digma* 2010 pag. 56.

Bianchi della Porta Manuel/Robert Vincent, «Responsabilité pénale de l'éditeur de médias en ligne participatifs», in: *medialex* 2009, pag. 19segg.

Boyd D.M./Ellison N.B., «Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication», 13(1), articolo 11, 2007 (**cit. Boyd D.M./Ellison N.B.**)

Egli Urs, «Soziale Netzwerke und Arbeitsverhältnis», in: *Jusletter* 17.01.2011.

Elixmann Robert, *Datenschutz und Suchmaschinen. Neue Impulse für den Datenschutz im Internet*, Berlino 2012.

Engel C./Knieps G., *Vorschriften des Telekommunikationsgesetzes über den Zugang zu wesentlichen Leistungen: Eine juristisch-ökonomische Untersuchung*, Baden-Baden 1998. (**cit. Engel C./Kniwps G.**)

Epiney Astrid/Fasnacht Tobias (ed.), *Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes*, Zurigo 2012.

European Network and Information Security Agency (ENISA), *The right to be forgotten – between expectations and practice*, Heraklion 2011.

Epiney Astrid/Probst Thomas/Gammenthaler Nina (ed.), *Datenverknüpfung. Problematik und rechtlicher Rahmen*, Zurigo 2011.

Hilty Lorenz/Oertel Britta/Wölk Michaela/Pärli Kurt, *Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern*, Zurigo 2012 (**cit. Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zürich 2012**).

Jöhri Yvonne, *Werbung im Internet: rechtsvergleichende, lauterkeitsrechtliche Beurteilung von Werbeformen*, Zurigo 2000 (**cit. Jöhri Yvonne, Werbung im Internet, Zurigo 2000**).

Keller Claudia, «AGB von Social-Media-Plattformen», in: *medialex* 2012 pag. 188 segg.

Latzer M./Just N./Metreveli S./Saurwein F. (2012). *Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project – Switzerland 2011*. Università di Zurigo, Zurigo.

Mayer-Schönberger Viktor, *Delete: Die Tugend des Vergessens in digitalen Zeiten*, Berlino 2010.

Meyer Julia, *Identität und virtuelle Identität natürlicher Personen im Internet*, Baden-Baden 2011.

Neuberger, Christoph, «Soziale Netzwerke im Internet. Kommunikationswissenschaftliche Einordnung und Forschungsüberblick». In: Neuberger, Christoph; Gehrau, Volker (ed.): *StudiVZ. Diffusion, Nutzung und Wirkung eines sozialen Netzwerks im Internet*. Wiesbaden 2011, pagg. 33 - 96.

Schmidt, Jan, «Was ist neu am Social Web? Soziologische und kommunikationswissenschaftliche Grundlagen». In: Zerfass, Ansgar; Welker, Martin; Schmidt, Jan (ed.): *Kommunikation, Partizipation und Wirkungen im Social Web*. Vol. 1. Colonia 2008, pagg. 18 - 40.

Schweizer Alex, «Data Mining – ein rechtliches Minenfeld. Rechtliche Aspekte von Methoden des Customer Relationship Management (CRM) wie Data Mining», in: *digma* 2001 pag. 108.

Schweizer Michael, «Das Recht am Wort nach Art. 28 ZGB», in: *medialex* 2011 pag. 197 segg.

Schweizer Michael, *Recht am Wort: Schutz des eigenen Wortes im System von Art. 28 ZGB*, Berna 2012 (**cit. Schweizer Michael, *Recht am Wort*, Berna 2012**).

Streiff Ullin/von Kaenel Adrian/Roger Rudolph, *Arbeitsvertrag Praxiskommentar*, 7. ed., Zurigo 2012.

Studer Melanie/Schweizer Matthias/Brucker-Kley Elke, «Sterben und Erben in der digitalen Welt», in: *Jusletter* 17.12.2012

Von Rimscha M. Björn, «Geschäftsmodelle für Social Media» . In: Petra Grimm und Oliver Zöllner (ed.): *Schöne neue Kommunikationswelt oder Ende der Privatheit? Die Veröffentlichung des Privaten in Social Media und populären Medienformaten*. Stoccarda 2012, pagg. 297–311.

Weber Rolf, *E-Commerce und Recht. Rechtliche Rahmenbedingungen elektronischer Geschäftsformen*, 2ª ed., Zurigo 2010.

Weber Rolf/Volz Stephanie, *Online Marketing und Wettbewerbsrecht*, Zurigo 2011.

10.3 Leggi

Legge federale del 15 dicembre 2000 sui medicamenti e i dispositivi medici **(**LATer); RS 812.

Legge federale del 13 dicembre 2002 sull’eliminazione di svantaggi nei confronti dei disabili (LDis); SR 151.3.

Legge federale del 19 giugno 1992 sulla protezione dei dati (LPD); RS 235.1.

Legge federale del 30 marzo 1911 di complemento del Codice civile svizzero (OR); RS 220.

Legge federale del 30 settembre 2011 sulla promozione delle attività extrascolastiche di fanciulli e giovani (LPAG); RS 446.1.

Legge federale del 21 giugno 1932 sulle bevande distillate (Legge sull’alcool); RS 680.

Legge federale del 18 dicembre 1987 sul diritto internazionale privato (LDIP); RS 291.

Legge federale del 20 giugno 2003 sul diritto penale minorile (DPMin); RS 311.1.

Legge federale del 6 ottobre 1995 sui cartelli e altre limitazioni della concorrenza (LCart); SR 251.

Legge federale del 24 marzo 2006 sulla radiotelevisione (LRTV); RS 784.40.

Legge federale del 19 dicembre 1986 contro la concorrenza sleale (LCSl); RS 241.

Legge federale del 9 ottobre 1992 sul diritto d'autore e sui diritti di protezione affini (LDA); RS 231.1.

Costituzione federale della Confederazione Svizzera del 18 aprile 1999 (Cost.); RS 101.

Legge sulle telecomunicazioni del 30 aprile 1997 (LTC); RS 784.10.

Convenzione del 4 novembre 1950 per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU); RS 0.101.

Codice penale militare del 13 giugno 1927 (CPM); RS 321.0.

Legge federale del 20 marzo 2009 di diritto processuale penale minorile (PPMin); RS 312.1.

Codice penale svizzero del 21 dicembre 1937 (CP); RS 311.0.

Codice civile svizzero del 10 dicembre 1907 (CC); RS 210.

Convenzione del 23 novembre 2001 sulla cibercriminalità; RS 0.311.43.

Convenzione del 30 ottobre 2007 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (CLug); RS 0.275.12.

Convenzione del 20 novembre 1989 sui diritti del fanciullo; RS 0.107.

Convenzione del 28 gennaio 1981 per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale; RS 0.235.1.

Convenzione n. 182 del 17 giugno 19999 concernente il divieto delle forme più manifeste di sfruttamento del fanciullo sul lavoro e l'azione immediata volta alla loro abolizione; RS 0.822.728.2.

Ordinanza del DFI del 23 novembre 2005 sulle bevande alcoliche; RS 817.022.110.

Ordinanza 5 del 28 settembre 2007 concernente la legge sul lavoro (Ordinanza sulla protezione dei giovani lavoratori, OLL 5); RS 822.115.

Ordinanza del 17 ottobre 2001 sulla pubblicità dei medicamenti (OPuM); RS 812.212.5.

Ordinanza del DEFR del 4 dicembre 2007 sui lavori pericolosi per i giovani; RS 822.115.2.

Ordinanza del 19 novembre 2003 sull'eliminazione di svantaggi nei confronti dei disabili (ODis); RS 151.31.

Ordinanza del 17 ottobre 2012 sulla promozione delle attività extrascolastiche di fanciulli e giovani (OPAG); RS 446.11.

Ordinanza del 23 novembre 2005 sulle derrate alimentari e gli oggetti d'uso (ODerr); RS 817.02.

Ordinanza del 9 marzo 2007 sulla radiotelevisione (ORTV); RS 784.401.

Ordinanza dell'11 giugno 2010 sui provvedimenti per la protezione dei fanciulli e dei giovani e il rafforzamento dei diritti del fanciullo; RS 311.039.1.

Ordinanza sui prodotti del tabacco e gli articoli per fumatori con succedanei del tabacco (OTab); RS 817.06.

10.4 Elenco dei riferimenti internazionali abbreviati

10.4.1 Consiglio d'Europa

Abridged Report of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS n. 108) - 29th Plenary Meeting del 10. dicembre 2012, T-PD (2012) RAP 29 Abr_en (**cit. Abridged Report of the Consultative Committee of Convention 108, T-PD (2012) RAP 29 Abr_en**).

Ad Hoc Advisory Group on Cross-Border Internet, 4th meeting, executive summary del 13. & 14.10.2011 (**cit. Ad Hoc Advisory Group on Cross-Border Internet**).

Recommandation Rec(2004)16 du Comité des Ministres aux Etats membres 15.12.2004 sur le droit de réponse dans le nouvel environnement des médias (**cit. Recommandation Rec(2004)16 sur le droit de réponse dans le nouvel environnement des médias**).

Raccomandazione Rec(2006)12 del Comitato dei ministri del Consiglio d'Europa agli Stati membri relativa alla responsabilizzazione dei bambini nel nuovo contesto dell'informazione e della comunicazione (**cit. Raccomandazione Rec(2006)12 relativa alla responsabilizzazione dei bambini nel nuovo contesto dell'informazione e della comunicazione**).

Raccomandazione CM/Rec(2007)2 del Comitato dei ministri del Consiglio d'Europa agli Stati membri, del 31 gennaio 2007, sul pluralismo dei mezzi d'informazione e la diversità dei loro contenuti (cit. **Raccomandazione CM/Rec(2007)2 sul pluralismo dei mezzi d'informazione e la diversità dei loro contenuti).**

Recommandation CM/Rec(2008)6 du Comité des Ministres du Conseil de l'Europe du 26.03.2008 sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet (**cit. raccomandazione CM/Rec(2008)6 sulle misure volte a promuovere il rispetto della libertà di espressione e di informazione con riguardo ai filtri Internet**).

Recommandation CM/Rec(2009)5 du Comité des Ministres aux Etats membres du 08.07.2009 visant à protéger les enfants contre les contenus et comportements préjudiciables et à promouvoir leur participation active au nouvel environnement de l'information et de la communication (**cit. Recommandation CM/Rec(2009)5 visant à protéger les enfants contre les contenus et comportements préjudiciables et à promouvoir leur participation active au nouvel environnement de l'information et de la communication**)

Recommandation CM/Rec(2010)13 du Comité des Ministres du Conseil de l'Europe aux Etats membres du 23.11.2010 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage (**cit. raccomandazione CM/Rec(2010)13 sulla protezione delle persone nell'ambito del trattamento automatico di dati personali per la creazione di profili**).

Recommandation CM/Rec(2011)7 du Comité des Ministres aux Etats membres sur une nouvelle conception des médias (**cit. Raccomandazione CM/Rec(2011)7 relativa a un nuovo concetto di media**).

Raccomandazione CM/Rec(2011)8 del Comitato dei ministri del Consiglio d'Europa del 21.09.2011 sulla protezione e promozione dell'universalità, integrità ed apertura di Internet (**cit. Raccomandazione CM/Rec(2011)8 sulla protezione e promozione dell'universalità, integrità ed apertura di Internet**).

Recommandation CM/Rec(2012)3 du Comité des Ministres aux Etats membres sur la protection des droits de l'homme dans le contexte des moteurs de recherche (**cit. La raccomandazione del Consiglio d'Europa per la protezione dei diritti dell'uomo nell'ambito dei motori di ricerca**).

Recommandation CM/Rec(2012)4 du Comité des Ministres du Conseil de l'Europe du 04.04.2012 sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux (**cit. Raccomandazione CM/Rec(2012)4 sulla protezione dei diritti dell'uomo nelle reti sociali**).

Déclaration du Comité des Ministres du Conseil de l'Europe du 07.12.2011 sur la protection de la liberté d'expression et de la liberté de réunion et d'association en ce qui concerne les plateformes internet gérées par des exploitants privés et les prestataires de services en ligne (**cit. dichiarazione sul rispetto della libertà di espressione, di riunione e di associazione in relazione alle piattaforme Internet gestite da soggetti privati e i fornitori di servizi Internet**).

Erklärung des Ministerkomitees des Europarats vom 21.09.2011 über die Grundsätze der Internet Governance (**cit. spiegazione dei principi che reggono la governance di Internet**).

Déclaration du 20.02.2008 du Comité des Ministres du Conseil de l'Europe sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur l'Internet (**cit. Déclaration du Conseil de l'Europe sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur l'Internet**).

Modernisation of Convention 108: New Proposals of The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS N. 108) del 27.04.2012, T-PD-BUR(2012)01Rev2_en (c**it. Modernisation of Convention 108, T-PD-BUR(2012)01Rev2_en**).

10.4.2 Unione europea

Parere del Gruppo 16/2011 di lavoro articolo 29 per la protezione dei dati adottato il 22 marzo 2012, **(**00727/12/IT WP 192), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2 (**cit. Parere del Gruppo di lavoro articolo 29 per la protezione dei dati 00727/12/IT WP 192**).

Relazione della commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sull'applicazione della raccomandazione del Consiglio, del 24 settembre 1998, concernente lo sviluppo della competitività dell'industria dei servizi audiovisivi e d'informazione europei attraverso la promozione di strutture nazionali volte a raggiungere un livello comparabile e efficace di tutela dei minori e della dignità umana, e della raccomandazione del Parlamento europeo e del Consiglio, del 20 dicembre 2006, relativa alla tutela dei minori e della dignità umana e al diritto di rettifica relativamente alla competitività dell'industria europea dei servizi audiovisivi e d'infor-

mazione in linea – Tutela dei minori nel mondo digitale –, COM(2011) 556 definitivo **(cit. Relazione della Commissione, COM(2011) 556 definitivo).**

Decisione n. 1351/2008/CE del Parlamento europeo e del Consiglio, del 16 dicembre 2008, relativa a un programma comunitario pluriennale per la protezione dei bambini che usano Internet e altre tecnologie di comunicazione, GU L 348 del 24.12.2008, pag. 118–127 (**cit. Decisione n. 1351/2008/CE relativa a un programma comunitario pluriennale per la protezione dei bambini che usano Internet e altre tecnologie di comunicazione**).

Raccomandazione del Parlamento europeo del 26 marzo 2009 destinata al Consiglio sul rafforzamento della sicurezza e delle libertà fondamentali su Internet, (2008/2160(INI)), GU C 117 E del 6.5.2010, pag. 206-213 (**cit. Raccomandazione del Parlamento europeo sul rafforzamento della sicurezza e delle libertà fondamentali su Internet, (2008/2160(INI)**).

Raccomandazione del Parlamento europeo e del Consiglio del 20.12.2006 relativa alla tutela dei minori e della dignità umana e al diritto di rettifica relativamente alla competitività dell'industria europea dei servizi audiovisivi e d'informazione in linea, 2006/952/CE, GU. L 378 del 27.12.2006 pagg. 72-77 (**cit. Raccomandazione relativa alla tutela dei minori e della dignità umana e al diritto di rettifica relativamente alla competitività dell'industria europea dei servizi audiovisivi e d'informazione in linea, 2006/952/CE**).

Decisione del Parlamento europeo del 15.122010 sull'influenza della pubblicità sul comportamento dei consumatori (2010/2052(INI)), GU C 169 E del 15.06.2012 pag. 58-65 (**cit. Decisione sull'influenza della pubblicità sul comportamento dei consumatori (2010/2052(INI)**).

Comunicazione della Commissione al Parlamento europeo, al Consiglio «Diritti umani e democrazia al centro dell'azione esterna dell'Unione europea — Verso un approccio più efficace» del 12.12.2011, COM(2011) 886 definitivo, (**cit. Comunicazione «Diritti umani e democrazia al centro dell'azione esterna dell'Unione europea — Verso un approccio più efficace, COM (2011) 866 definitivo**).

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al comitato economico e sociale e al Comitato delle regioni intitolata «Relazione sulla competitività digitale in Europa: principali risultati della strategia i2010 nel periodo 2005-2009» del 04.08.2009, (COM(2009) 390 definitivo (**cit. «Relazione sulla competitività digitale in Europa: principali risultati della strategia i2010 nel periodo 2005-2009» (COM(2009) 390 definitivo**).

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al comitato economico e sociale e al Comitato delle regioni «Strategia europea per un'internet migliore per i ragazzi» del 02.05.2012, COM(2012) 196 definitivo (**cit. Comunicazione della Commissione «Strategia europea per un'internet migliore per i ragazzi», COM(2012) 196 definitivo**).

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al comitato economico e sociale e al Comitato delle regioni intitolata «Valutazione intermedia del programma pluriennale dell'Unione per la protezione dei minori che usano internet e le altre tecnologie di comunicazione», del 03.02.2012, COM(2012) 33 definitivo (**cit. Comunicazione della Commissione «Valutazione intermedia del programma pluriennale dell'Unione per la protezione dei minori che usano internet e le altre tecnologie di comunicazione», COM(2012) 33 definitivo**).

Comunicazione della Commissione al Consiglio e al Parlamento europeo «Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica» del 28.03.2012, COM(2012) 140 definitivo (**cit. Comunicato stampa della Commissione europea del 28.03.2012 «Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica», IP/12/317 COM(2012) 140 definitivo)**.

Direttiva 2011/83/UE del Parlamento europeo e del Consiglio del 25 ottobre 2011 sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE del Par-

lamento europeo e del Consiglio e che abroga la direttiva 85/577/CEE del Consiglio e la direttiva 97/7/CE del Parlamento europeo e del Consiglio, GU L 304 del 22.11.2011 pagg. 64-88 (**cit. Direttiva 2011/83/UE sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE e che abroga la direttiva 85/577/CEE e la direttiva 97/7/CE**).

Direttiva 95/46/CE del Parlamento europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU. L 281 del 23/11/1995 pag. 31-50 (**cit. Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati**).

Conclusioni del Consiglio, dell'11 maggio 2012, sulla promozione delle potenzialità di creatività e d'innovazione dei giovani, GU c 169 del 15.06.2012 pag. 1-4 (**cit. Conclusioni del Consiglio, dell'11 maggio 2012, sulla promozione delle potenzialità di creatività e d'innovazione dei giovani, 2012/C 169/01**).

Parere del Comitato economico e sociale europeo «L'Internet degli oggetti» GU C 77 del 31.3.2009 pag. 60-63 (cit. **Parere «L'Internet degli oggetti» 2009/C 77/15**).

Parere del Comitato delle regioni «Un'agenda digitale europea», GU C 015 del 18.01.2011, pag. 34-40 (**cit. Parere «Un'agenda digitale europea», 2011/C 15/07**).

Parere del Comitato economico e sociale europeo sul tema «Utilizzo responsabile delle reti sociali e prevenzione dei disturbi a queste associati», GU C 352 del 15.11.2012 pag. 31-35 (**cit. Parere del Comitato economico e sociale europeo sul tema «Utilizzo responsabile delle reti sociali e prevenzione dei disturbi a queste associati, 2012/C 351/07**).

Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) del 25.01.2012, COM(2012) 11 definitivo (**cit. Proposta UE di regolamento generale sulla protezione dei dati, COM(2012) 11 definitivo**).

10.4.3 Germania

Antwort der Bundesregierung auf die kleine Anfrage «Rechtsextremismus im Internet» del 07.06.2010, stampa 17/1930 (**cit. Antwort Bundesregierung auf Anfrage «Rechtsextremismus im Internet», 17/1930**).

Gesetzesentwurf des Bundesrates zur Änderung des Telemediengesetzes del 03.08. 2011, stampa 17/6765 (**cit. Progetto di modifica della legge sui mezzi di telecomunicazione, 17/6765**).

Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes vom 15.12.2010, stampa 17/4230 (**cit. Disegno di legge sulla protezione dei dati dei collaboratori, 17/4230**).

10.5 Studi & rapporti

Bernet ZHAW Studie Social Media Schweiz 2012.

Rapporto «Portale pubblico sulla salute» di e-health Suisse.

ENISA Threat Landscape Report del 28.09.2012.

EU Kids Online Final Report, settembre 2011.

Rapporto annuale 2011 Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI).

Studio Optimus «Sexuelle Übergriffe an Kindern und Jugendlichen in der Schweiz», febbraio 2012.

Fondazione Warentest «Datenschutz bei Onlinenetzwerken», 2010.

Studio dell'Ufficio federale di statistica «Internet nelle economie domestiche della Svizzera: primi risultati della rilevazione Omnibus TIC 2010».

Cifre inedite tratte dallo Studio netTEEN (Perren S. & Sticca F., 2012. Jacobs Center for Productive Youth Development, Università di Zurigo).

Fondazione Wikimedia: Rapporto annuale 2010/2011.