educa.Guides

Protezione dei dati
Privacy a scuola

Scuola e ICT

Avvertenze legali

Editore educa.ch

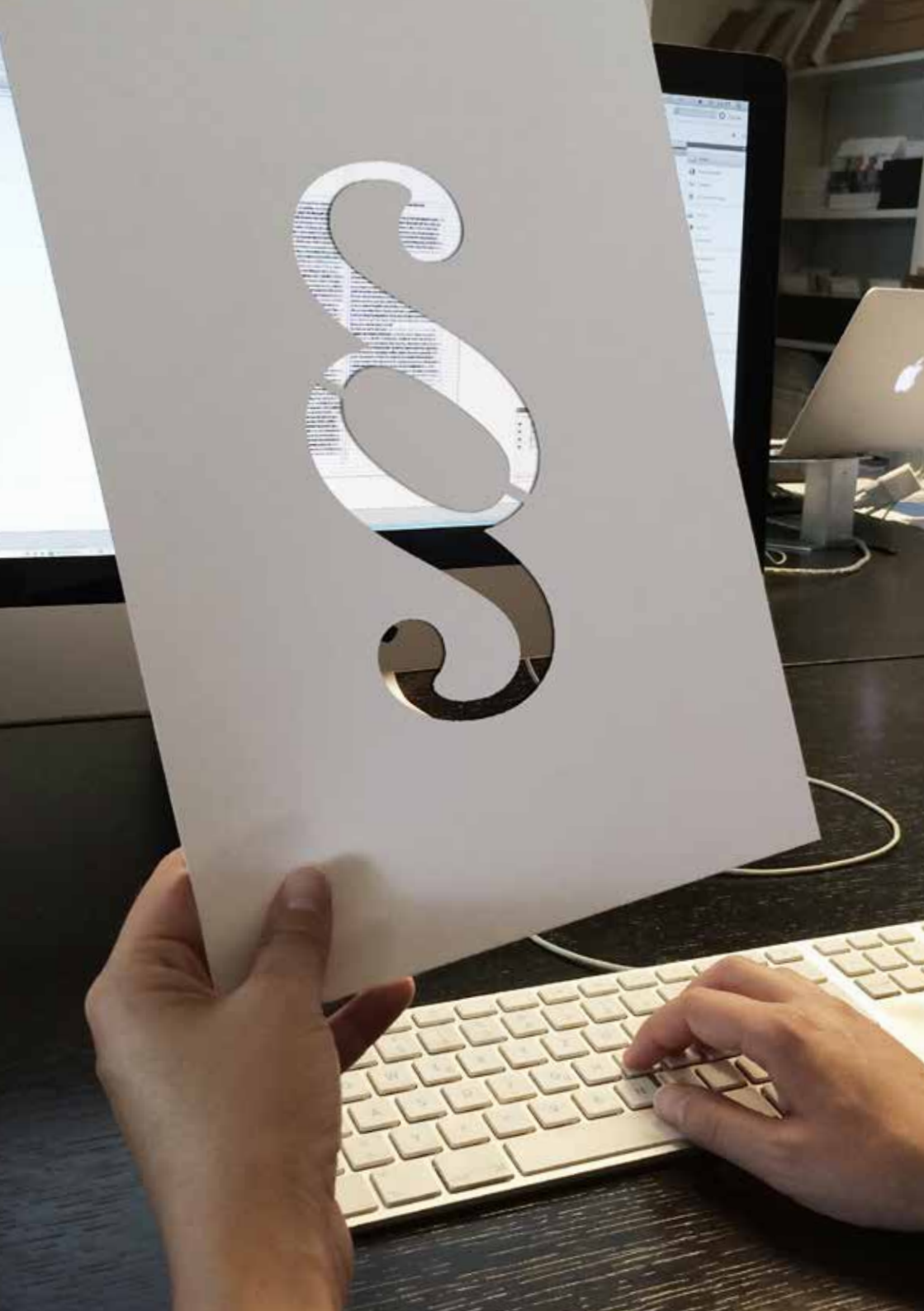
Estratti riprodotti con la gentile autorizzazione della/dell':
- Direzione della pubblica istruzione del Canton Berna:
  Linee direttrici sulla protezione dei dati personali nelle scuole del Canton Berna (documento di riferimento)
- Incaricato federale della protezione dei dati e della trasparenza (IFPDT):
  Protezione dei dati, Observations concernant les sites de réseautage social, Qualche indicazione di sicurezza su WLAN

Fotografie büro z {grafik design}, Bern

Novembre 2009

A questa guida corrisponde una pagina Internet di educa.ch, sulla quale trovate il file PDF della guida stessa per la sua consultazione online e per raccogliere ulteriori informazioni e link relativi a siti che propongono materiale pedagogico in tema. Queste informazioni e questi link vengono aggiornati regolarmente. Le date di pubblicazione o di eventuali revisioni della guida sono indicate nel PDF.

→ Sito web



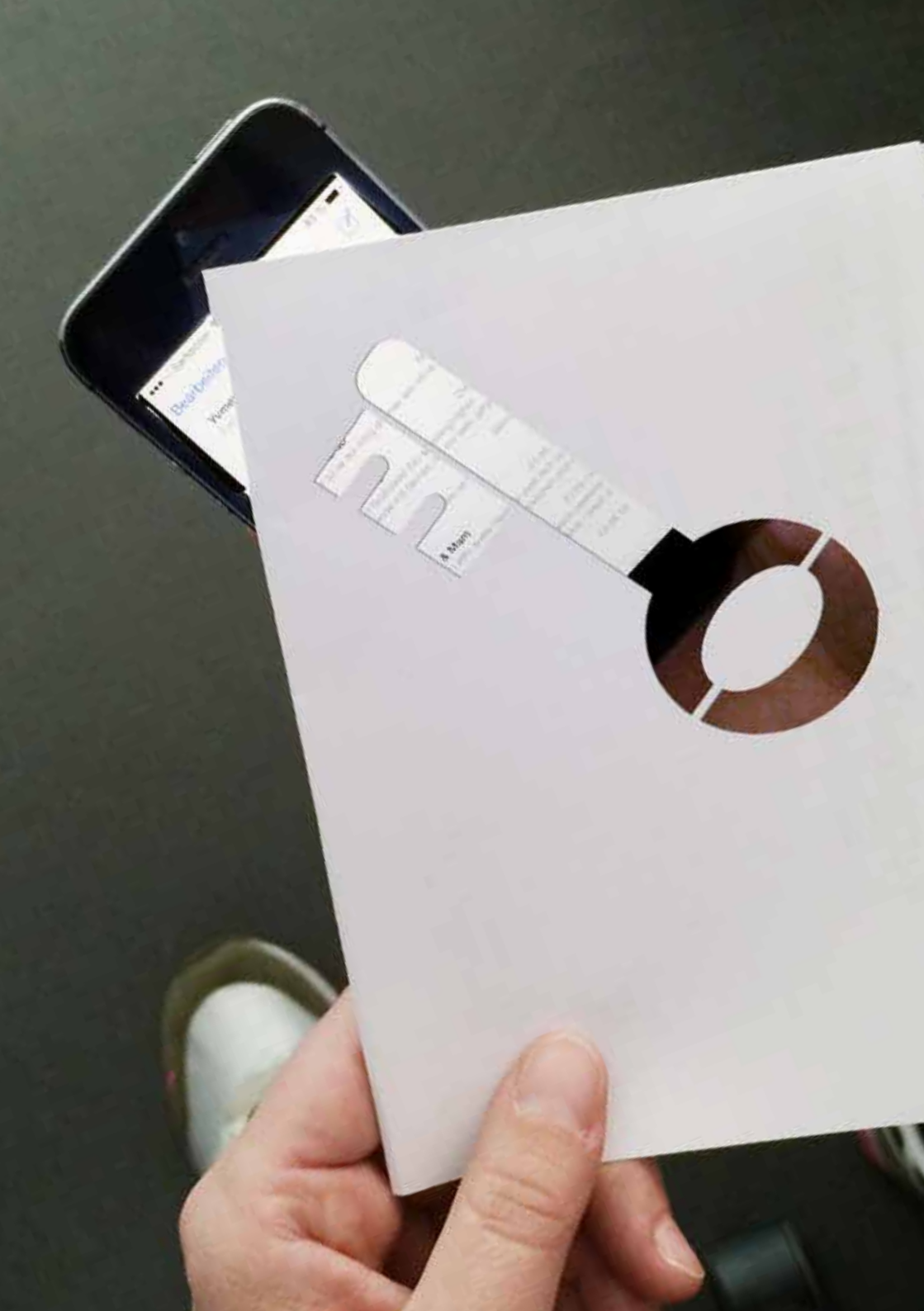
Introduzione

«Protezione dei dati» non significata soprattutto la protezione dei dati in sé, come erroneamente può far pensare il termine, bensì la protezione delle persone dall'abuso dei loro dati personali nella vita quotidiana. Con l'arrivo nelle classi delle applicazioni Web 2.0, la protezione dei dati personali degli allievi – ma anche degli insegnanti – acquista un'importanza sempre maggiore. Purtroppo molti insegnanti non sono abbastanza consapevoli dell'estrema attualità del tema della protezione dei dati. Infatti, prima dell'avvento del Web 2.0, erano soprattutto le amministrazioni e le autorità scolastiche ad occuparsi di questo argomento, per esempio per il trasferimento ad altri uffici dei dati personali relativi agli allievi. Ora però il tema della protezione dei dati riguarda tutti coloro che sono attivi nelle scuole, perché ormai nessuno vuole più rinunciare del tutto ai servizi interattivi di Internet.

Giornata europea della protezione dei dati

La giornata europea della protezione dei dati, promossa dal Consiglio d'Europa, ricorre il 28 gennaio e ha lo scopo di spiegare ai cittadini come vengono trattati i loro dati personali e quali sono i loro diritti in questo ambito.

→ coe.int



Concetti fondamentali

Il primo capitolo è un'introduzione al tema della protezione dei dati. Vengono fornite le risposte alle seguenti domande: quali dati sono considerati degni di protezione? Dove è disciplinata legalmente la protezione dei dati?

Diritto all'autodeterminazione dell'informazione
Il cosiddetto diritto all'autodeterminazione dell'informazione costituisce un principio importante del nostro ordine sociale. L'autodeterminazione dell'informazione significa che ogni individuo deve avere il più possibile la facoltà di decidere quali informazioni che lo riguardano possono essere comunicate, quando e a chi.

A cosa serve la protezione dei dati?

Semplificando, si potrebbe affermare che il primo obiettivo della protezione dei dati è quello di difendere il diritto all'autodeterminazione dell'informazione della persona.

Si tratta però di un compito non sempre facile, perché a volte esistono anche interessi legittimi a limitare questo diritto di autodeterminazione, ad esempio nel caso di indagini della polizia.

Proporzionalità
Fondamentalmente la protezione dei dati deve assicurare che in ogni singolo caso di trattamento dei dati sia mantenuta la proporzionalità, ovvero che in nessun caso siano raccolti più dati di quelli assolutamente necessari per di un determinato incarico limitato nel luogo e nel tempo. Inoltre, deve essere garantito che la persona interessata abbia la possibilità di controllare il più possibile il trattamento dei dati che lo riguardano ed eventualmente di impedirlo.

Diritto di consultazione dei documenti
Per questo è imprescindibile che ognuno abbia la possibilità di farsi rendere conto dai detentori delle banche dati quali informazioni sulla propria persona sono da loro trattate. A tal fine, la legge sulla protezione dei dati stabilisce il diritto di consultare i propri dati personali che può essere fatto valere nei confronti dei detentori delle collezioni di dati.

Dove e come è definita legalmente la protezione dei dati?

L'art. 13 della Costituzione federale stabilisce il principio, secondo il quale ognuno ha diritto al rispetto della sua vita privata e familiare, della sua abitazione, della sua corrispondenza epistolare, delle sue relazioni via posta e telecomunicazioni nonché di essere protetto da un impiego abusivo dei suoi dati personali.

La protezione dei dati, quindi, non è volta a tutelare i dati in sé, ma i diritti fondamentali delle persone.

Legge federale sulla protezione dei dati
Per fondare legalmente questa tutela, è stata approvata la legge federale sulla protezione dei dati (LPD), che è in vigore dal 1° luglio 1993. La relativa ordinanza (OLPD) disciplina i dettagli.

La legge sulla protezione dei dati (LPD) è rivolta all'Amministrazione federale, nonché a tutte le persone private che trattano dati personali.

Leggi cantonali sulla protezione dei dati
Inoltre, anche in altre leggi esistono numerose norme sulla protezione della personalità. Per esempio, negli articoli 28–28l del Codice civile si stabilisce come procedere legalmente in caso di lesione della personalità.

Le leggi cantonali sulla protezione dei dati disciplinano il trattamento dei dati da parte delle amministrazioni e costituiscono la base per i regolamenti sulla protezione dei dati dei Comuni. Questi a loro volta sono la base per le scuole gestite dai Comuni.

Dati personali

I dati personali sono informazioni riguardanti una determinata persona. Con «informazioni» si intende qualsiasi informazione. Queste comprendono le constatazioni di fatto e i giudizi di valore, indipendentemente dalla tecnologia (codici analogici o digitali, parole, immagini, audio o una combinazione di questi) e indipendentemente dalla modalità di comunicazione (tra persone presenti, per posta o trasmissione elettronica). Invece, non sono incluse le conoscenze di una persona che non sono scritte o registrate. Se le informazioni sono private del nome e di tutti gli altri elementi che permettono di associarle a una persona determinata, queste non sono più dati personali.

Trattamento dei dati personali
Il «trattamento» comprende qualsiasi utilizzo dei dati personali, in modo particolare la raccolta, la conservazione, la modifica, l'associazione, la comunicazione e la distruzione.

Comunicazione dei dati personali
Con la «comunicazione» dei dati personali, si intende la messa a disposizione di dati personali, in particolare la concessione della consultazione, il fornire ragguagli, la diffusione e la pubblicazione.

Dati personali «degni di particolare protezione»
Per i «dati personali degni di particolare protezione» è necessaria una cautela speciale.
I dati personali «degni di particolare protezione» sono:
– informazioni sulle opinioni religiose, ideologiche o politiche, l'appartenenza e l'attività
– informazioni sulla sfera segreta, specialmente sulle condizioni spirituali, affettive e fisiche
– informazioni sulla necessità di aiuti sociali o sulla dipendenza dall'assistenza
– informazioni su indagini di polizia e procedimenti penali in corso ecc.

Riprese e registrazioni
In linea di massima non sono considerati dati personali «degni di particolare protezione». Queste sono degne di particolare protezione solo se contengono una delle informazioni citate sopra (ovvero se, per esempio, nelle immagini sono visibili i sintomi di una malattia oppure se in base alle immagini si possa desumere l'appartenenza religiosa).

Anche se le riprese e le registrazioni per se stesse non sono «degne di particolare protezione», questo non significa che nel trattamento di riprese e registrazioni che contengono solo dati personali «normali» non sia necessaria molta cautela. Anche la pubblicazione di immagini di persone su Internet può avere conseguenze gravi e difficilmente valutabili sui diritti di personalità dei soggetti interessati, per esempio a causa dell'abuso delle immagini su altri siti web, la diffamazione delle persone rappresentate con programmi per l'elaborazione delle immagini ecc.


AF-L
AF-L
OK

Rischi nell'insegnamento con le ICT

Questo capitolo è rivolto in modo particolare agli insegnanti e agli allievi. Vengono presentati i pericoli derivanti dell'utilizzo di servizi Internet interattivi, le cosiddette applicazioni Web 2.0. Alla fine del capitolo segue una lista di raccomandazioni per l'uso delle applicazioni Web 2.0 rivolta a tutte le persone attive nella scuola.

Mancanza di consapevolezza in materia di sicurezza

La tecnologia dell'informazione permette di registrare un'enorme quantità di dati personali e di metterli in relazione. Purtroppo la consapevolezza in materia di sicurezza di chi si occupa del trattamento dei dati spesso non regge il passo con le innovazioni tecnologiche. Inoltre, la maggior parte delle persone – che si trattati degli addetti al trattamento dei dati o delle persone i cui dati sono trattati – non sono ancora abbastanza sensibilizzati sulle questioni riguardanti la protezione della personalità. Spesso si trattano i propri dati personali in modo troppo imprudente, sia su Internet sia nel compilare i formulari di sondaggi o concorsi, solo per citare due esempi.

Navigazione, reti sociali, chat

Le utenti e gli utenti di Internet non sono più meri «consumatori» che cercano e scaricano le informazioni messe a disposizione dai provider su siti web statici, ma utilizzano Internet interattivamente e contribuiscono dinamicamente ai siti web. Questo sviluppo è riassunto nel termine Web 2.0.

In questo contesto sono nati numerosi siti di social networking (Social Networking Sites, SNS). Si tratta di ampi portali, dove le utenti e gli utenti registrati si incontrano, stringono «amicizie» e scambiano informazioni, fotografie e video.

Gli SNS pongono la protezione dei dati dinnanzi a nuove sfide. Le leggi in materia di protezione dei dati in origine erano concepite per tutelare i dati personali dal trattamento illegittimo o esagerato da parte dello Stato e in seguito da parte delle imprese commerciali. Con gli SNS sono emersi due nuovi aspetti fondamentali:

– le informazioni personali sono inserite nei profili Internet dagli stessi utenti e quindi con il loro consenso;
– i cittadini privati hanno ampio accesso ai dati personali di altre persone. Questo può comportare molteplici rischi.

Utilizzo di dati personali negli SNS

Gli SNS offrono molti vantaggi sociali, come per esempio la possibilità di praticare networking, stabilire contatti al di là dei confini nazionali o pubblicare i propri contenuti. L'intenzione di questa informativa non è quindi di condannare per principio gli SNS. L'obiettivo è piuttosto sensibilizzare le autorità e gli utenti a usare le informazioni personali nei social network nel rispetto della protezione dei dati. Infatti, anche se i servizi di social networking il più delle volte sono gratuiti, non si tratta comunque di istituzioni senza scopo di lucro. Si tratta di uno «scambio»:

i servizi sono messi a disposizione delle utenti e gli utenti in cambio dei loro dati. Dietro a questi portali si nasconde una grande forza di mercato, società internazionali che sotto la pressione degli investitori e degli azionisti devono generare profitti sempre maggiori. L'unica merce che questi servizi di social networking possono offrire ai propri investitori sono i dati personali, e la quotazione in borsa degli SNS dice tutto sul valore reale di tali dati.

Rischi e pericoli

L'utilizzo delle reti sociali nasconde molti pericoli noti. I malintenzionati possono, infatti, sfruttare a proprio vantaggio le prerogative specifiche dei sistemi di social network (SNS), tra queste anche la nuova interpretazione dei concetti di fiducia e confidenzialità. Laddove l'amicizia assume sempre più una connotazione quantitativa, è facile – simulando fatti o persino sotto mentite spoglie – diventare «amico» di qualcuno per entrare in possesso di informazioni che probabilmente un interlocutore non rivelerebbe mai in una conversazione a tu per tu. La tesi sostenuta da questo tipo di reti, secondo cui non si farebbe altro che trasferire in Internet la comunicazione quotidiana tra amici, suggerisce un senso di intimità che invece non è garantito, tanto più se gli ostacoli all'accesso alla rete sono pochi.

Chi utilizza imprudentemente i siti di social networking senza prendere le dovute precauzioni si espone a rischi di vario genere.

Account utenti, profili
È praticamente impossibile cancellare definitivamente gli account. Questo innanzi tutto perché vengono in parte solo «disattivati» e non rimossi e secondariamente perché gli utenti attivi lasciano su altre pagine del portale molte informazioni supplementari praticamente impossibili da cancellare. Gli utenti finiscono così per perdere il controllo sui propri dati.

Dati personali
Internet non dimentica: qualsiasi programma può memorizzare i dati inseriti nei profili e nelle bacheche degli utenti. Si moltiplicano così le collezioni private di dati personali, che permettono di gestire i dati tramite la catalogazione secondo determinati criteri per mezzo della funzione di ricerca. Questo aumenta il rischio che le informazioni siano utilizzate a fini diversi da quelli previsti inizialmente. Se divulgati al di fuori dei siti di social networking i dati possono arrecare grave pregiudizio alla persona interessata.

Metadati
I provider dei siti di social networking hanno accesso non solo ai dati personali, bensì anche ai metadati. In molti casi, però, non è chiaro l'uso che gli operatori di SNS fanno di tali dati, come per esempio la durata della connessione, la localizzazione dell'indirizzo IP, il tempo di permanenza e i percorsi di navigazione sul sito ecc. Dai dati personali e i metadati insieme si possono ottenere profili molto particolareggiati degli utenti.

Fotografie, immagini

Le fotografie che ritraggono persone riconoscibili e ne riportano i nomi consentono di identificare in maniera univoca i soggetti immortalati. Per mezzo di appositi software per il riconoscimento facciale si possono ispezionare i siti di social networking e altre piattaforme simili alla ricerca di specifiche persone, che con questo sistema possono essere identificate anche quando desiderano rimanere anonime (ad es. su un sito di incontri), oppure si può associare una fotografia pubblicata su un SNS al curriculum vitae consultabile sul sito di un'azienda.

CBIR

Un rischio simile deriva dalla possibilità di utilizzare tecniche di content based image retrieval (CBIR), ovvero il recupero di immagini basato sul contenuto: il riconoscimento automatico di caratteristiche di oggetti o luoghi raffigurati nelle immagini, ad es. un quadro o una casa, consente di localizzare geograficamente la situazione ritratta in una foto, favorendo la divulgazione di un indirizzo, il proliferare di atteggiamenti persecutori (lo stalking) o altri atti criminali.

Collegamenti

Alcuni SNS consentono collegamenti più allargati con profili o indirizzi elettronici di altre persone, non necessariamente membri della comunità, senza per altro chiederne il consenso. Questa opportunità rappresenta un rischio per la sfera privata di ognuno di noi.

Single Sign On

Gli utenti di molti SNS hanno la possibilità di semplificare il metodo di gestione delle loro caselle di posta elettronica inserendole in un'unica applicazione web. In questo modo è possibile visualizzare contemporaneamente tutti i messaggi associati al proprio profilo con un solo nome utente e una sola password. Tutto questo può essere molto pratico, ma fa sorgere dubbi sulla sicurezza.

Atti criminali

Nella maggior parte dei casi, registrarsi in un SNS comporta ostacoli minimi: basta infatti fornire alcuni dati personali che, non essendo sottoposti a verifica, possono tranquillamente essere inventati. Una volta registrati, può risultare estremamente facile stabilire nuovi contatti ed entrare a fare parte della cerchia di amici di altre persone. Questo comporta notevoli rischi di infiltrazione in queste comunità a scopi discutibili o addirittura criminali.

Furto d'identità

Il furto d'identità è un gioco da ragazzi: basta aprire un profilo utilizzando il nome di una persona famosa per poi sfruttarne la notorietà a proprio vantaggio oppure diffamarla ostentando un atteggiamento disdicevole. Oppure è possibile allestire un profilo a nome di una persona che si vuole danneggiare appartenente al proprio ambiente scolastico o al vicinato, ridicolizzandola o inviando cattiverie firmate a suo nome.

Tra le forme di utilizzo abusivo dei dati può essere annoverato il cosiddetto phishing, il furto di dati a scopi criminali, nonché il cyberstalking e il cyberbullismo.

Phishing

Il phishing consiste nel furto di dati mediante l'utilizzo di email o moduli web falsi: l'utente è indotto a credere di inserire le informazioni in un modulo affidabile (per esempio della sua banca), quando in realtà sta fornendo i suoi dati personali (per esempio login, password, codice TAN, codici PIN ecc.) a un ladro di dati.

Cyberstalking
Il cyberstalking è un vecchio fenomeno in veste nuova: le possibilità di contatto elettronico messe a disposizione dai siti di social networking possono essere sfruttare a fini malevoli per molestare una persona. Inoltre, vista la notevole quantità di dati personali divulgati volontariamente dagli stessi utenti, è possibile che i malintenzionati riescano a recuperare l'indirizzo della loro vittima e scoprirne le abitudini per perseguitarla nel mondo reale.

Cyberbullismo
Anche il cyberbullismo è la versione presente su Internet di un fenomeno reale di vecchia data. L'aggressore può nascondersi dietro un falso profilo, restando dunque anonimo, e sfruttare il meccanismo insito negli SNS per importunare o umiliare qualcuno. Questo, inoltre, può avvenire sotto gli sguardi di altri membri della comunità, così da rendere ancora più pesante il danno inflitto alla vittima.

Raccomandazioni agli utenti e alle direzioni scolastiche

Utenti
- Utilizzate nomi utenti e password differenti per i diversi servizi.
- Selezionate per il vostro profilo le impostazioni conformi alla protezione dei dati. Consentite l'accesso alle informazioni e alle fotografie solo a una cerchia ristretta di persone. Non pubblicate su Internet contenuti sensibili.
- Negli SNS siate cauti nel pubblicare i vostri dati personali (nome, indirizzo, numero di telefono) e altre informazioni personali (per esempio, le vostre opinioni politiche). Utilizzare pseudonimi.

– Prima di pubblicare delle informazioni, domandatevi sempre se vorreste essere confrontati con questi dati durante un colloquio di lavoro – anche tra dieci anni.
– Rispettate la sfera privata delle altre persone, non pubblicate i loro dati personali e non aggiungete il loro nome nelle fotografie.
– Informatevi sul gestore del portale e sulle modalità di protezione della sfera privata degli utenti. Il servizio dispone di una certificazione sulla protezione dei dati e sulla sicurezza?
– Leggete le condizioni di contratto. Osservate criticamente il comportamento del gestore.

Direzioni scolastiche

– Gli utenti dei servizi di social networking devono essere sensibilizzati ai rischi che vi sono connessi tramite apposite campagne.
– Attenzione con i divieti: invece di proibire l'uso di SNS, le scuole dovrebbero permetterlo (parzialmente); in questo modo le attività di social networking non si svolgeranno completamente fuori controllo. Allo stesso tempo è possibile informare gli alunni, gli insegnanti e i genitori.

Linee guida europee sulla protezione dei dati

Della tematica dei social network si sono occupati a fondo molti organi europei di controllo della protezione dei dati.

Per maggiori informazioni consultate i seguenti siti:

→ European Network and Information Security Agency ENISA. Position Paper No. 1: Security Issues and Recommendations for Online Social Networks. (PDF)
Editore: Giles Hogben, ottobre 2007.

→ Rapporto e Linee-Guida in materia di privacy nei servizi di social network «Memorandum di Roma», Marzo 2008

Email

Campi degli indirizzi
Spesso nei campi «A» o «Cc» delle email che ci arrivano nella casella di posta elettronica figurano tutti i destinatari del messaggio. Per motivi di trasparenza, si può trattare di una scelta assolutamente ragionevole, se per esempio i destinatari partecipano ad un medesimo progetto o se comunque si conoscono già. Tuttavia, a seconda del contenuto e della situazione, la comunicazione di tutti i destinatari può risultare inopportuna, specialmente se i riceventi non si conoscono. In tal caso, il mittente deve utilizzare l'opzione «Bcc» (blind carbon copy). Così facendo, i singoli destinatari non possono sapere quali altre persone hanno ricevuto la comunicazione.

Raccomandazione
Quando i destinatari di una email non si conoscono personalmente, inserire sempre gli indirizzi nel campo «Bcc».

Rischio di spam e phishing
Va ricordato inoltre che la diffusione di indirizzi email aumenta il rischio di spam e di attacchi di phishing: in quest'ultimo caso, una email contraffatta contenente istruzioni e link può indurre il destinatario a credere di comunicare con un mittente affidabile.

Raccomandazione
Ignorate le email che contengono istruzioni e link.

Blog

La legge sulla protezione dei dati vieta la divulgazione di dati concernenti terzi senza il consenso scritto della persona interessata.

Raccomandazione

Se in un blog trovate informazioni sul vostro conto e volete che siano cancellate, rivolgetevi per prima cosa all'autore tramite il modulo di contatto o via email. Se questo non sortisce alcun effetto, contattate il provider del blog. Non pubblicate in nessun caso un commento in merito all'informazione che vi riguarda. Questo sarebbe controproducente, perché attirerebbe l'attenzione dei lettori proprio sull'informazione sgradita.

Anche nel caso del proprio blog personale è facile cedere alla tentazione di rivelare informazioni sul proprio conto, senza essere consapevoli dei rischi che questo comporta. La divulgazione volontaria di informazioni sul proprio conto non pone problemi dal punto di vista della normativa sulla protezione dei dati personali. Ciononostante, essa può comportare le conseguenze negative citate anche a proposito delle reti sociali.

Norme di comportamento

Le seguenti regole di comportamento costituiscono una protezione contro le possibili conseguenze negative derivanti dai blog personali:

– per evitare che il vostro blog privato acquisti una notorietà eccessiva, limitate i lettori a cui vi rivolgete. Sfruttate a tal fine le diverse possibilità di proteggere l'intero blog o singoli interventi con una password o di limitare il diritto d'accesso a determinati ospiti;

– utilizzate sempre uno pseudonimo e non rivelate dettagli che permettono di risalire alla vostra identità, alle abitudini, al luogo di soggiorno o residenza, al datore di lavoro ecc.;
– utilizzate le tecnologie di anonimizzazione. Invisiblog, per esempio, offre un servizio di hosting per blog gratuito e anonimo. Per evitare che il vostro indirizzo IP possa essere identificato, utilizzate la rete TOR (→ Wikipedia). Inoltre, esistono numerosi fornitori di software specializzati in sistemi di anonimizzazione, come → anonymizer.com;
– se volete rimanere anonimi quando segnalate il vostro blog ai motori di ricerca, utilizzate un server ping. Pingomatic.com offre questo tipo di servizio;
– impedite che i motori di ricerca trovino il vostro blog, utilizzando un file di testo robots (robots.txt);
– registrate anonimamente il vostro nome a dominio. Per esempio, Online Policy Group (OPG) offre la registrazione anonima.

Consigli

«Chi vuole, può muoversi anonimamente su Internet senza problemi, trasmettendo i propri dati solo in modo criptato.

Navigazione: utilizzando la rete Tor (→ torproject.org), si possono criptare tutti i dati.

Condivisione di file: tramite le reti come Bittorrent si possono scaricare file anonimamente, per esempio con il servizio gratuito Bit Blinder (→ bitblinder.com) oppure a pagamento con provider come Torrent Privacy (→ torrentprivacy.com).

Email: qualsiasi provider serio permette la trasmissione sicura delle email tramite «https:» e con PGP si possono criptare i testi».

Fonte: Christian Bütikofer, Tagesanzeiger 18.07.2009

Fotocamere digitali e integrate nei telefonini

Riprese e registrazioni illecite da parte di allievi o da parte dei genitori

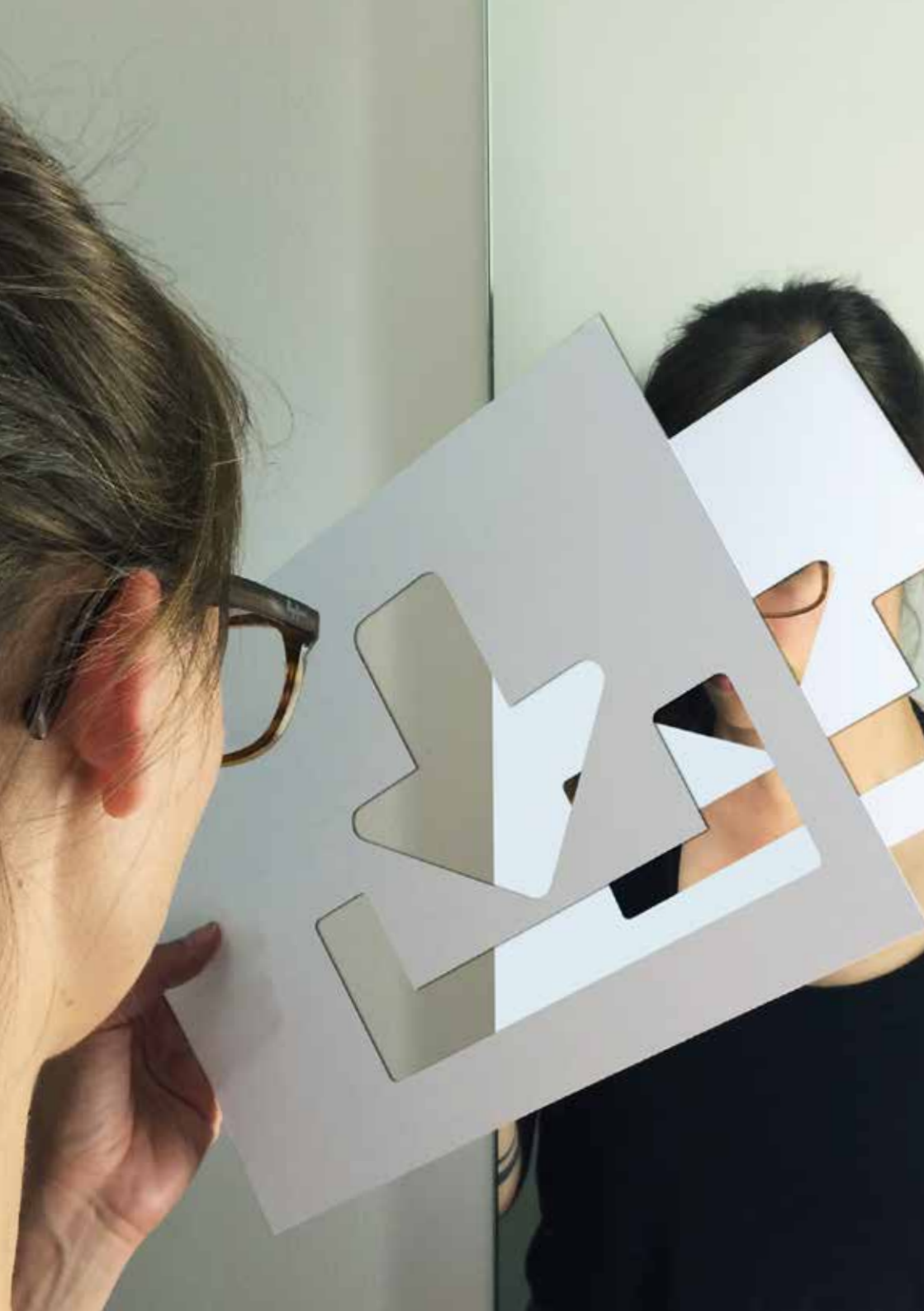
Le allieve e gli allievi, così come i loro genitori, in quanto cittadini privati sono tenuti al rispetto della legge federale sulla protezione dei dati. Questa vieta le riprese e le registrazioni che non sono autorizzate da un consenso personale, una legge o da un interesse preponderante pubblico o privato. Di norma le riprese e le registrazioni violano i diritti della personalità, soprattutto quando sono commentate e pubblicate su Internet (per esempio su siti web o blog di allieve e allievi). Per questo, inoltre, le allieve e gli allievi devono essere informati dagli insegnanti e dalle direzioni scolastiche che la diffamazione, la calunnia e l'ingiuria costituiscono reato.

Registrazioni da parte di genitori durante gli eventi scolastici

Le registrazioni da parte dei genitori in occasione di eventi scolastici (feste, rappresentazioni teatrali, manifestazioni sportive, giorni di visita a scuola o settimane di escursione ecc.) sono inerenti al rapporto giuridico tra il bambino registrato (o i suoi genitori) e la persona che esegue la registrazione. Si tratta dunque principalmente di una questione di diritto privato. Se i genitori sono informati dell'evento aperto al pubblico o agli altri genitori e fintanto che gli insegnanti non riscontrano gravi violazioni della legge (per esempio, quando i genitori con le loro riprese molestano altri bambini), non sussiste alcun obbligo di intervenire contro la registrazione eseguita dai genitori. In linea di massima spetta ai soggetti ripresi o fotografati (o ai loro genitori) tutelare i propri diritti e opporsi alle registrazioni illecite.

Visite inattese alla classe di singoli genitori

Nel caso di visite inattese alla classe di singoli genitori non sono ammesse registrazioni, visto che, diversamente dagli eventi scolastici, gli altri genitori non ne sono informati e non possono far valere i propri diritti. Dal punto di vista del diritto della protezione dei dati, le persone soggette a riprese e registrazioni illegittime possono adottare misure giudiziarie per la protezione della personalità. In casi estremi si può pretendere la cancellazione immediata delle registrazioni e, in caso di rifiuto, provvedere da sé alla cancellazione.



Indicazioni per l'amministrazione scolastica

Questo capitolo si rivolge in primo luogo alle direzioni scolastiche, illustrando i principi del diritto in materia di protezione dei dati. Inoltre, viene richiamata l'attenzione in modo particolare sugli aspetti del diritto sulla protezione dei dati in relazione alla gestione dei dati personali di allievi e insegnanti con l'utilizzo di tecnologie basate sul web. Alla fine segue un capito più prettamente tecnico sul tema delle reti WLAN e della sicurezza.

Protezione dei dati e segreto d'ufficio

In qualità di collaboratori di istituti pubblici, gli insegnanti e le direzioni scolastiche esercitano una funzione di servizio pubblico. Essi sono quindi equiparatati a membri delle autorità e nella loro funzione sono sottoposti alle norme della relativa legge cantonale sulla protezione dei dati. Inoltre, le norme penali in materia di segreto d'ufficio (art. 320 CP) obbligano gli insegnanti al rispetto della personalità delle allieve e degli allievi.

Segreto d'ufficio

Le norme penali in materia di segreto d'ufficio obbligano i collaboratori di istituti pubblici a non rivelare segreti d'ufficio. Un segreto d'ufficio è un fatto non generalmente noto, di cui un membro di un'autorità è venuto a conoscenza nell'esercizio delle sue funzioni.

Da un lato le norme sul segreto d'ufficio si applicano ad un ambito più esteso rispetto alle norme sulla protezione dei dati, comprendendo anche i dati non personali. Dall'altro il loro campo d'applicazione è più ristretto, perché disciplinano solo la comunicazione di segreti e non la registrazione, la conservazione, la distruzione ecc. di dati.

Gli insegnanti sono dunque tenuti a non rivelate i «segreti», di cui sono venuti a conoscenza nell'esercizio della loro funzione. La loro comunicazione, tuttavia, può essere giustificata da una delega o un obbligo legislativo.

Segreto professionale

Il segreto d'ufficio va distinto dal segreto professionale in base all'art. 321 del Codice penale. Anche in questo caso lo scopo è la protezione di segreti, ma non da parte di membri delle autorità, bensì da parte di determinate categorie professionali, specialmente ecclesiastici, avvocati, notai, medici, dentisti, farmacisti e levatrici. Alcune categorie di persone sono tenute al rispetto di entrambi gli obblighi di segretezza, come per esempio i medici scolastici.

Leggi cantonali sulla protezione dei dati

Le leggi cantonali sulla protezione dei dati regolano la condotta delle autorità cantonali nel trattamento dei dati personali. Sono disciplinati la raccolta, la conservazione, la modifica, l'associazione, la comunicazione e la distruzione dei dati personali. I dati che non contengono riferimenti a persone non rientrano nel campo d'applicazione di tali leggi. Se le disposizioni legislative sono infrante da collaboratori di istituti pubblici, la persona interessata può pretendere, tramite apposita domanda, che i dati errati o raccolti illecitamente siano corretti o cancellati. Inoltre, la violazione del diritto in materia di protezione dei dati (per esempio la comunicazione illecita di dati personali o la perdita di dati personali che devono essere

conservati) può determinate misure disciplinari interne (p.es. una nota di biasimo). Se in aggiunta la violazione è causa di un danno, può dare luogo all'obbligo di risarcimento da parte della scuola (di norma risponde il Comune) o – in caso di danni causati intenzionalmente o per negligenza grave – da parte dell'insegnante.

Dati raccolti ad uso personale dell'insegnante
I dati personali trattati dall'insegnante esclusivamente per uso proprio non sono sottoposti alla legge sulla protezione dei dati. Si tratta del materiale di lavoro personale dell'insegnante, come gli appunti per la preparazione di un colloquio con i genitori o le note in agenda. L'esclusione di tali informazioni dalla legge sulla protezione dei dati nega alle persone interessate il diritto di accedervi. Ciò non significa, però, che questi dati possano essere divulgati. Anche il materiale di lavoro personale deve dunque essere protetto dall'accesso da parte di terzi e non può essere lasciato incustodito. Se per esempio un appunto di un colloquio contiene informazioni sensibili riguardante un allievo, questo deve essere custodito nella cattedra o in un armadio chiuso a chiave. I dati personali comprendono anche le verifiche di apprendimento, se queste possono essere attribuite ad allieve o allievi. Se le informazioni sono private del nome e di tutti gli altri elementi che permettono di associarle a un determinato allievo, non si tratta di più di dati personali.

Principi del diritto in materia di protezione dei dati

Le disposizioni delle leggi cantonali sulla protezione dei dati sono rivolte a tutte le autorità del Cantone. Esse quindi non sono concepite specificamente per il trattamento dei dati personali nelle scuole. Per questo è importante conoscere i principi della legge sulla protezione dei dati. Da questi, infatti, devono essere ricavate le soluzioni concrete per la realtà scolastica.

Legittimità del trattamento dei dati personali
Il trattamento dei dati personali deve essere sempre legittimo. La legge sulla protezione dei dati distingue i dati personali «normali» da quelli «degni di particolare protezione» (vedi sopra). Semplificando, la differenza sta nel fatto che il trattamento dei dati personali «degni di particolare protezione» è sottoposto a regole più rigide rispetto a quello di dati personali «normali».

Trattamento dei dati personali normali
I dati personali «normali» possono essere trattati,
– se una legge (è sufficiente una base a livello di ordinanza) lo autorizza; oppure se
– se il trattamento è necessario per l'adempimento di compiti prescritti per legge (vale a dire che senza il trattamento dei dati, l'adempimento del compito prescritto per legge sarebbe gravemente ostacolato).

Trattamento dei dati personali degni di particolare protezione
I dati personali «degni di particolare protezione» possono essere trattati
– se ciò è espressamente previsto da una legge (in questo caso è necessaria una base a livello di legge); oppure se
– se ciò è assolutamente necessario per l'adempimento di un compito prescritto per legge (vale a dire che l'adempimento del compito prescritto per legge sarebbe impossibile senza il trattamento dei dati); oppure se
– se la persona interessata dà il suo consenso.

Principio di limitazione delle finalità
I dati raccolti in ambito scolastico conformemente alle regole suddette possono essere trattati solo per gli scopi per cui sono stati raccolti o per finalità prevedibili dagli allievi e dai genitori. Nella scuola tali scopi sono determinatati dai compiti citati sopra della scuola dell'infanzia e della scuola dell'obbligo.

Per questo motivo non è possibile cedere gli elenchi delle classi per fini commerciali.

Principio della proporzionalità
In base a questo principio, come già accennato, i dati personali possono essere trattati solo se necessario per l'adempimento di un compito prescritto per legge. Raccogliere i dati al fine di conservarli (per esempio, la raccolta di dati il cui scopo al momento del rilevamento non è chiaro) è illegale. Inoltre, il principio della proporzionalità impone di scegliere tra le varie possibilità di trattamento dei dati sempre quella che garantisce la minore intromissione possibile nei diritti di personalità della persona interessata.

Principio della buona fede
Dal principio della buona fede consegue che il trattamento dei dati deve essere evidente e trasparente. Il trattamento segreto dei dati è dunque proibita. Le allieve e gli allievi, così come i genitori, devono poter sapere senza troppi sforzi quali dati personali sono trattati. Per questo i dati personali normalmente devono essere raccolti tramite le allieve e gli allievi interessati o i titolari del diritto di custodia e non attraverso altre persone o autorità.

Principio di esattezza
Questo principio dà alle allieve e agli allievi, così come ai genitori, il diritto di richiedere la rettifica o la distruzione dei dati personali inesatti sul loro conto.

Sicurezza dei dati
Chi tratta i dati personali è responsabile della loro sicurezza.

Requisiti per il consenso al trattamento dei dati
Il consenso può essere la base per la legittimità del trattamento dei dati. Tuttavia, il consenso al trattamento dei dati dovrebbe riguardare solo una situazione determinata, limitata nel luogo e nel tempo e non dovrebbe essere concesso una volta per tutte o autorizzare il trattamento a tempo indeterminato. Normalmente la persona interessata è l'allieva o l'allievo. Poiché il consenso può essere concesso solo da persone con capacità di discernimento, va chiarito quali requisiti siano necessari per considerare gli allievi capaci di giudicare. Devono poi essere esaminati i requisiti formali del consenso. In base al Codice civile, è capace di discernimento qualunque persona che non sia priva della facoltà di agire ragionevolmente per effetto della sua età infantile o di «infermità o debolezza mentale, di ebbrezza o di uno stato consimile». Questo significa che un bambino o un adolescente è capace di giudicare, se è in grado di avere una propria volontà e di agire di conseguenza. La legge non stabilisce alcun limite fisso di età. A seconda del livello di sviluppo, l'adolescente può avere un diverso orizzonte delle esperienze. Gli allievi della scuola dell'infanzia e della scuola dell'obbligo di norma hanno un'età compresa tra i 4 e i 16 anni. In questo periodo di tempo la capacità di avere una volontà propria e di agire di conseguenza varia. Anche tra coetanei tale facoltà può essere sviluppata in modo diverso.

Fondamentalmente, però, può essere affermato quanto segue:
Se valutare le conseguenze del trattamento dei dati spesso non è semplice nemmeno per gli adulti, per bambini tale compito risulta ancora più difficoltoso. Per questo motivo, in merito al trattamento dei dati personali «degni di particolare protezione» e di quelli «normali», la loro capacità di discernimento può essere riconosciuta tutt'al più nel periodo finale della scuola pubblica. Prima è consigliabile chiedere il consenso di chi esercita la patria podestà. Un bambino

può valutare le conseguenze del trattamento dei dati e avere una propria volontà solo in casi molto chiari e semplici.

Consenso

Il consenso può essere orale o scritto, esplicito o tacito. Per il trattamento di dati personali «normali» che non costituiscono un rischio rilevante per le persone interessate, può essere sufficiente il tacito consenso. Si suppone il tacito consenso, in mancanza di opposizione contro il trattamento dei dati previsto da regolamenti o reso generalmente noto. Quando possibile il consenso dovrebbe essere chiesto in forma scritta, in modo da poter costituire una prova.

Dati personali per Internet provider, fornitori di software ecc.

In generale la diffusione dei dati è permessa solo nella misura in cui ciò è consentito espressamente dal Comune nel regolamento sulla protezione dei dati. Normalmente i regolamenti modello in materia di protezione dei dati ne vietano la comunicazione per fini commerciali. Tuttavia, le ordinanze di alcuni Comuni premettono espressamente questo tipo di comunicazione dei dati. In presenza di una tale ordinanza, la comunicazione è permessa (per esempio, art. 3 comma 1 del regolamento sulla protezione dei dati del Comune di Thun).

Informazioni sugli elenchi

Le informazioni sugli elenchi sono dati ordinati sistematicamente, per esempio elenchi di nomi, indirizzi o indirizzi email di tutti gli allievi di una scuola oppure di tutti gli esercenti la patria podestà degli allievi di una scuola. Di massima tali elenchi possono essere distribuiti solo se ciò è espressamente autorizzato da un regolamento sulla protezione dei dati. Le persone interessate, però, devono essere informate prima della prima comunicazione per dare loro la possibilità di far valere interessi preminenti. Questa procedura è raccomandata soprattutto quando sussiste il sospetto che i dati personali possano essere usati illecitamente.Qualora per la diffusione dei dati si necessiti del consenso di chi esercita la patria podestà o delle allieve e degli allievi, è necessario richiedere attivamente l'esplicita autorizzazione per iscritto. Non devono essere utilizzate formulazioni come «in assenza di indicazioni contrarie … presumiamo il suo consenso». [BL: promemoria sulla protezione dei dati]

Richieste per fini commerciali

Le richieste – specialmente da parte di fornitori di servizi web – devono essere trattate con attenzione. In ogni caso devono essere lette attentamente le condizioni generali di contratto dei fornitori di servizi web (per esempio provider software-as-a-service). Infatti, ciò che nel prospetto pubblicitario si presenta come un'offerta allettante per la scuola, potrebbe essere legato a condizioni che creano dipendenze indesiderate o che sono problematiche sul piano della protezione dei dati.

Siti web delle scuole

La messa a disposizione su Internet di dati riguardanti le allieve e gli allievi o gli insegnanti corrisponde al trattamento dei dati personali. Dunque anche in questo caso devono essere rispettati i principi citati. I dati pubblicati su Internet sono accessibili in tutto il mondo e possono essere usati lecitamente e illecitamente per varie finalità. Per questo è necessario usare molta cautela, soprattutto per le immagini. Inoltre, devono essere rispettati i requisiti di sicurezza in Internet.

Direttive per i siti web delle scuole
Di regola i dati seguenti possono essere pubblicati senza problemi:
Informazioni prive di riferimenti a persone:
– Agenda scolastica
– Organizzazione scolastica
– Linee guida
– Indirizzi di istituzioni vicine alla scuola
– Regolamenti scolastici
Relazioni prive di riferimenti a persone:
– eventi scolastici e di classe
– rappresentazioni teatrali
– feste scolastiche
– settimane tematiche
– escursioni
Lavori di allieve e allievi, se non sono riconducibili a loro

Dati riguardanti le allieve e gli allievi, gli insegnanti, così come i membri delle commissioni e autorità scolastiche

In generale, se le persone interessate non concedono o ritirano il loro consenso alla pubblicazione di qualsiasi dato personale – anche per i cosiddetti dati non problematici – il loro diritto di rimozione delle informazioni deve essere soddisfatto immediatamente e il contenuto in questione deve essere prontamente cancellato dal sito web.

Dati non problematici

Di norma, i seguenti dati non sono problematici:

- cognome
- nome
- funzione

Necessità di previo esplicito consenso volontario

I seguenti dati personali sensibili non possono essere pubblicati senza previo esplicito consenso volontario:

- indirizzi privati
- indirizzi email
- immagini di persone, se queste sono identificabili
- indicazioni su hobby e materie preferite
- lavori di allievi con riferimenti alla persona

Dati sensibili

Nonostante il previo esplicito consenso volontario, è necessario evitare di pubblicare sul sito web della scuola i seguenti dati:

- indirizzi privati
- numeri di telefono
- indirizzi email
- immagini di persone identificabili

Link
I link non possono condurre a pagine illecite, per esempio, pagine a contenuto pornografico, razzista o diffamatorio. Tutti i link devono essere controllati periodicamente.

Webcam
Va evitato l'uso di webcam per la trasmissione di immagini di persone identificabili.

Moduli di contatto
Se il sito web mette a disposizione un contatto via email o tramite modulo web, deve essere indicato che il collegamento non è sicuro e che non dovrebbero essere trasmesse informazioni riservate.

Registrazione delle visite, cookie
La registrazione dei visitatori del sito è vietata. Se il sito impiega i cookie, deve essere dichiarato lo scopo.

Guestbook, forum
Guestbook e forum non possono essere utilizzati, se i terzi possono inserire direttamente sul sito i loro contributi senza il controllo della scuola. La scuola deve evitare possibili diffamazioni da parte di terzi.

Indicazioni di sicurezza per le reti WLAN

WLAN sta per wireless local area network, cioè rete locale senza fili. Le reti WLAN servono specialmente per la connessione a Internet degli apparecchi mobili negli hotel, nei ristoranti, nelle stazioni ferroviarie, nelle abitazioni e nelle aziende. Le reti WLAN collegano i computer, le stampanti, gli scanner e altri apparecchi e permettono spesso anche la connessione a Internet. Gli apparecchi sono collegati tra loro tramite cosiddetti access point. La WLAN è standardizzata dalla IEEE (→ Wikipedia: IEEE).

Le reti WLAN sono molto diffuse nelle aziende e nelle abitazioni private, perché permettono una grande flessibilità senza grovigli di cavi e con un'elevata velocità di trasmissione. La portata del segnale tra l'access point e gli apparecchi, a seconda della potenza di trasmissione e la qualità dei muri, varia da pochi metri a diverse dozzine di metri.

Gli innegabili vantaggi tecnici delle reti WLAN d'altro canto rendono necessarie particolari misure tecniche e organizzative. Infatti, il segnale è accessibile nell'intera zona coperta dalla rete WLAN, cioè anche da terzi non autorizzati. In primo luogo si tratta quindi di proteggere i dati riservati, impedendo l'accesso a terzi. In secondo luogo deve essere impedito ad altri di approfittare della rete WLAN per la connessione a Internet, riducendone la larghezza di banda, o addirittura di sfruttarla per atti illegali.

Misure di sicurezza

La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI della Confederazione propone le seguenti misure concrete per la sicurezza e la protezione dei dati:

- modificare la password standard per la amministrazione dell'access point;
- se possibile, amministrare l'access point tramite cavo, p. es. ethernet, e disattivare la funzione di amministrazione senza fili;
- disattivare eventuali funzioni per l'amministrazione a distanza via Internet dell'access point;
- modificare l'identificazione di rete (SSID) e disattivare l'emissione dell'identificazione di rete (SSID Broadcast) per fare sì che l'access point rimanga nascosto agli estranei;
- attivare la cifratura più potente supportata dall'access point e dalle apparecchiature terminali (preferibilmente WPA 2 o WPA). Utilizzare la chiave più lunga o una password potente. Il vecchio standard Wired Equivalent Privacy (WEP) non offre una sicurezza sufficiente e non dovrebbe più essere impiegato;
- se la rete lo permette e se si dispone delle necessarie competenze, impiegare indirizzi IP statici invece di DHCP (Dynamic Host Configuration Protocol);
- impiegare un filtro MAC per limitare l'accesso alla rete WLAN a determinati apparecchi terminali;
- se l'access point dispone della relativa funzione e il funzionamento della rete non è compromesso, ridurre la potenza di trasmissione per limitare la portata della rete WLAN;
- attivare la rete WLAN solo quando necessario.

Link utili sul tema delle rete WLAN

→ MELANI: Wireless LAN
→ UFSP: WLAN
→ Wikipedia: Wi-Fi Protected Access

educa.ch
Istituto svizzero dei media per la formazione e la cultura
Erlachstrasse 21 | Casella postale 612 | CH-3000 Berna 9

Telefono: +41 (0)31 300 55 00
info@educa.ch | www.educa.ch