1. Minori: la sua foto finisce sul quotidiano on line, ma la sposa bambina non è lei

Il Garante per la privacy ha dato ragione ad un padre che si era rivolto all'Autorità per tutelare il diritto all'immagine e all'identità personale della figlia minore [doc. web n. 7354837].

Oggetto della segnalazione una foto della bimba, ritratta vestita da sposa nell'atto di infilare un anello nuziale nella mano di un adulto, pubblicata sulla pagina web di una testata online a corredo di un articolo che riguardava una ragazzina ridotta in schiavitù dal padre e promessa in sposa ad un connazionale dietro pagamento di una somma di denaro.

La bambina fotografata però non era quella a cui si riferiva l'articolo ma la figlia del segnalante, che era stata ritratta in abito matrimoniale per una campagna di sensibilizzazione contro la pratica delle spose bambine promossa da una ong internazionale. La testata on line dunque aveva utilizzato la foto in un contesto improprio, che poteva indurre i lettori a ritenere che la minore ritratta fosse la vera protagonista del fatto di cronaca.

L'associazione della fotografia della bambina protagonista della campagna di sensibilizzazione, figlia del segnalante, configura - secondo il Garante - un trattamento illecito di dati personali. L'accostamento, infatti, dell'immagine al fatto di cronaca è lesivo del diritto all'identità personale della minore (artt. 2 e 11 e 137 del Codice privacy) e può arrecare un danno alla bambina fotografata e la cui immagine era stata diffusa con obiettivi del tutto diversi. La testata, inoltre, non ha adottato alcun accorgimento per prevenire l'identificazione della minore, ad es., pixelandone il volto. Una misura che, se richiesta (in astratto) rispetto alla eventuale diffusione della foto della vera protagonista della vicenda (art. 7 del codice deontologico dei giornalisti e Carta di Treviso), a maggior ragione si sarebbe dovuta adottare per la figlia del segnalante che nulla ha a che vedere con i fatti di cronaca riportati nell'articolo.

All'editore della testata, che nel corso dell'istruttoria ha rimosso la fotografia dal sito, l'Autorità ha prescritto di adottare le misure necessarie affinché l'immagine non sia ulteriormente utilizzata in violazione del diritto all'identità personale della bambina.

2. Avvocati e crediti formativi: ok al riconoscimento via webcam. Il sistema non prevede l'uso di dati biometrici per la verifica dell'identità dei partecipanti ai corsi online

Via libera del Garante privacy ad un sistema informatico che consente di verificare l'effettiva corrispondenza tra l'identità degli avvocati iscritti a corsi di formazione professionali, erogati in streaming, a quella delle persone effettivamente connesse [doc. web n. 6826368]. Il sistema, sottoposto a verifica preliminare dell'Autorità, è finalizzato a evitare che alcuni partecipanti pongano in essere comportamenti sleali per farsi attribuire crediti formativi simulando la partecipazione ai corsi a distanza.

Secondo quanto dichiarato dalla società il controllo dell'identità avverrà acquisendo, a intervalli casuali durante lo svolgimento del corso, la fotografia dei partecipanti collegati in diretta streaming, mediante la webcam del pc di ciascun professionista. Al termine dell'evento le immagini acquisite verranno inserite nelle schede personali insieme al diagramma di connessione.

Successivamente un operatore confronterà le fotografie con quelle dei documenti di identità raccolti in fase di iscrizione, mediante un'operazione che non comporta alcun trattamento biometrico, non essendo prevista la verifica automatizzata di immagini digitali. Il Garante ha richiamato a tale proposito la definizione di riconoscimento facciale elaborata dal Gruppo Art. 29 secondo cui "il riconoscimento facciale è il trattamento automatizzato di immagini digitali contenenti i volti degli individui allo scopo di identificarli, verificarne l'identità o categorizzarli".

L'Autorità ha ritenuto lecito il trattamento dei dati personali che dovrà essere oggetto di una specifica e articolata informativa che consenta agli interessati l'esercizio dei diritti, espliciti le finalità e le modalità del trattamento, descriva le caratteristiche tecniche del sistema ed evidenzi i tempi di conservazione dei dati personali.

Il Garante ha prescritto inoltre alla società di raccogliere dagli interessati uno specifico consenso informato al trattamento delle immagini e di configurare il sistema in modo da trattare i dati nel rispetto dei principi di proporzionalità, necessità e correttezza. La società dovrà consentire l'accesso ai dati personali acquisiti solo a soggetti adeguatamente formati, designati "responsabili" e "incaricati" del trattamento, e dovrà adottare idonee misure di sicurezza a tutela della privacy degli interessati.

3. No all'algoritmo della reputazione, viola la dignità della persona

No del Garante privacy alla banca dati on line della reputazione [doc. web n. 5796783]. Il progetto per la misurazione del "rating reputazionale", elaborato da una organizzazione articolata in un'associazione e da una società preposta alla gestione dell'iniziativa, viola le norme del Codice sulla protezione dei dati personali e incide negativamente sulla dignità delle persone.

L'infrastruttura, costituita da una piattaforma web e un archivio informatico, dovrebbe raccogliere ed elaborare una mole rilevante di dati personali contenuti in documenti "caricati" volontariamente sulla piattaforma dagli stessi utenti o "pescati" dal web. Attraverso un algoritmo, il sistema assegnerebbe poi ai soggetti censiti degli indicatori alfanumerici in grado, secondo la società, di misurare in modo oggettivo l'affidabilità delle persone in campo economico e professionale.

Nel disporre il divieto di qualunque operazione di trattamento presente e futura, il Garante ha ritenuto che il sistema comporti rilevanti problematiche per la privacy a causa della delicatezza delle informazioni che si vorrebbero utilizzare, del pervasivo

impatto sugli interessati e delle modalità di trattamento che la società intende mettere in atto. Pur essendo infatti legittima, in linea di principio, l'erogazione di servizi che possano contribuire a rendere maggiormente efficienti, trasparenti e sicuri i rapporti socioeconomici, il sistema in esame - realizzato peraltro in assenza di una idonea base normativa - presuppone una raccolta massiva, anche on line, di informazioni suscettibili di incidere significativamente sulla rappresentazione economica e sociale di un'ampia platea di individui (clienti, candidati, imprenditori, liberi professionisti, cittadini). Il "rating reputazionale" elaborato potrebbe ripercuotersi sulla vita delle persone censite, influenzando le scelte altrui e condizionando l'ammissione degli interessati a prestazioni, servizi o benefici.

Per quanto riguarda, poi, l'asserita oggettività delle valutazioni, la società non è stata in grado di dimostrare l'efficacia dell'algoritmo che regolerebbe la determinazione dei "rating" al quale dovrebbe essere rimessa, senza possibilità di contestazione, la valutazione dei soggetti censiti. L'Autorità nutre, in generale, molte perplessità sull'opportunità di rimettere ad un sistema automatizzato ogni decisione su aspetti così delicati e complessi come quelli connessi alla reputazione. Senza contare, infatti, la difficoltà di misurare situazioni e variabili non facilmente classificabili, la valutazione potrebbe basarsi su documenti e certificati incompleti o viziati, con il rischio di creare profili inesatti e non rispondenti alla identità sociale delle persone censite.

Dubbi sono stati espressi dal Garante anche sulle misure di sicurezza del sistema - basate, prevalentemente, su sistemi di autenticazione "debole" (user id e password) e su meccanismi di cifratura dei soli dati giudiziari secondo l'Autorità davvero inadeguate, specie se rapportate all'elevato numero di soggetti che potrebbero essere coinvolti e all'ingente quantitativo di informazioni, anche molto delicate, che verrebbero registrate all'interno della piattaforma.

Ulteriori criticità, infine, sono state ravvisate nei tempi di conservazione dei dati e nell'informativa da rendere agli interessati.

4. Volto e voce per l'accesso ai cedolini on line: sì al test

Sì del Garante privacy alla sperimentazione di un progetto pilota di autenticazione basato sul riconoscimento vocale e facciale per la consegna dei cedolini on line [doc. web n. 5763201]. Il Consorzio per il Sistema Informativo (Csi) Piemonte potrà testare in un contesto "reale" e per un periodo di tempo limitato una app installata sugli smartphone di quei dipendenti che accetteranno di utilizzarla per accedere al servizio "cedolini on line", in alternativa al sistema in uso basato su user id e password.

I "volontari", tramite la app, potranno visualizzare e scaricare il cedolino mensile, il modello CU, la posizione assicurativa per chi aderisce al Fondo pensione. Il test consentirà al Consorzio di verificare l'accuratezza, la facilità d'uso e la sicurezza, anche sotto il profilo dei dati personali, del servizio di autenticazione biometrica.

Il progetto che è stato sottoposto a verifica preliminare dell'Autorità rientra nell'ambito del programma europeo PIDaaS (Private Identity as a Service) e ha solo finalità scientifiche. L'ok del Garante si riferisce esclusivamente alla fase sperimentale e non riguarda eventuali future applicazioni "a regime" del sistema che dovranno essere sottoposte a un nuovo vaglio dell'Autorità.

Per innalzare il livello di protezione dei dati dei partecipanti al test il Garante ha prescritto l'adozione di ulteriori misure rispetto a quelle già previste dal Csi. In primo luogo, il Consorzio dovrà fare in modo che la sperimentazione non coinvolga meccanismi e applicativi aziendali utilizzati nella gestione del rapporto di lavoro. Gli utenti che decideranno di aderire alla sperimentazione (dalla quale potranno recedere in qualsiasi momento) dovranno quindi accedere ad una installazione di test creata ad hoc, contenente solo i loro cedolini.

Il Consorzio, inoltre, dovrà fornire agli aderenti all'iniziativa apposite credenziali e un indirizzo di posta elettronica temporaneo per avere accesso alla sezione della intranet da cui si avvia la fase di registrazione per effettuare il login alla app. I dati biometrici poi, dovranno essere cancellati in modo irreversibile al termine della sperimentazione o su richiesta del partecipante.

Infine, poiché il progetto prevede la comunicazione di alcuni dati ad un partner spagnolo il Consorzio dovrà individuare i termini e le condizioni delle operazioni di comunicazione e del trattamento dei dati conferiti al partner, compresi gli aspetti relativi alla sicurezza. Eventuali incidenti informatici o di violazioni dei dati biometrici (data breach) dovranno essere comunicati tempestivamente al Garante, e, nei casi previsti, agli utenti.

5. Cronaca: garantire sempre riservatezza bambino malato
Il minore va tutelato da forme di comunicazione lesive dell'armonico sviluppo della sua personalità

No a troppe informazioni che rendono identificabile un bambino malato. Il diritto del minore alla riservatezza prevale sul diritto di cronaca e neanche il consenso dei genitori autorizza il giornalista a riportare informazioni che possano nuocere al suo sviluppo. Lo ha ribadito [doc. web n 5029484] il Garante privacy nel definire un'istruttoria avviata d'ufficio a seguito della pubblicazione su alcune testate di diversi dati identificativi di una bambina (fotografie, il nome, il luogo di residenza, l'età, il nome e il cognome della madre, il nome della scuola frequentata), associati a precise indicazioni della patologia di cui soffre. Il Garante ha tuttavia ritenuto di non dover adottare alcun provvedimento inibitorio, poiché le testate, appena avuta notizia dell'avvio dell'istruttoria, hanno eliminato gli articoli dalla rete o oscurato i dati che rendevano identificabile la bambina.

La vicenda descritta negli articoli affronta, a parere dell'Autorità, un tema di indubbio interesse pubblico, riguardando il dibattito in corso sul rapporto rischi benefici delle vaccinazioni. Nel riportare la notizia, i giornalisti devono però tener conto delle regole che disciplinano il rapporto tra attività giornalistica e protezione dei dati

personali e delle garanzie poste a tutela dei più piccoli. In particolare, quelle del codice deontologico e della Carta di Treviso che considerano il diritto del minore alla riservatezza primario rispetto al diritto di cronaca e stabiliscono che in caso di bambini malati, il giornalista deve porre "particolare attenzione e sensibilità nella diffusione delle immagini e delle vicende" per evitare forme di sensazionalismo lesive della loro personalità.

E, anche se in questo caso la diffusione di dati personali è avvenuta con il consenso dei genitori, questo elemento, sottolinea l'Autorità, non è di per sé sufficiente a legittimare l'identificabilità del minore. Il consenso parentale non esime infatti il giornalista dal valutare il potenziale pregiudizio che può derivare dalla pubblicazione di informazioni così dettagliate. Il giornalista è chiamato ad adottare le cautele di volta in volta più opportune per tutelare il minore, senza per questo abdicare al ruolo fondamentale di denuncia e informazione della collettività. Tale principio, più volte affermato dall'Autorità, trova conferma anche nella Carta di Treviso, secondo cui, "a prescindere dall'eventuale consenso dei genitori, il minore non va coinvolto in forme di comunicazioni lesive dell'armonico sviluppo della sua personalità".

6. No al riconoscimento facciale per ottenere finanziamenti

Il Garante della privacy ha vietato l'uso di un sistema di riconoscimento facciale che avrebbe dovuto registrare e verificare i volti di chi richiede un finanziamento allo scopo di prevenire possibili furti di identità.

La società che aveva progettato il servizio prevedeva di acquisire - tramite scansione - la fotografia presente sul documento di identità dei potenziali clienti al momento in cui richiedevano mutui, prestiti o altre forme di finanziamento presso istituti di credito o altri intermediari finanziari. I dati biometrici del volto - inseriti in una banca dati e associati con altre informazioni personali - sarebbero stati poi confrontati con quelli già censiti o presenti in altri archivi, ad esempio per l'identificazione di soggetti ricercati. La ricerca sarebbe poi stata estesa anche a immagini pubblicate sulla stampa e su internet.

Nel corso dell'istruttoria per la verifica preliminare del progetto sottoposto alla sua attenzione, l'Autorità ha innanzitutto evidenziato che non può ritenersi necessario e proporzionato un uso generalizzato e incontrollato dei dati biometrici dei clienti che, tra l'altro, si possono prestare a utilizzi impropri e possibili abusi.

Il Garante, inoltre, ha individuato molteplici criticità relative al nuovo sistema, che peraltro avrebbe comportato la raccolta dei volti di un numero enorme di persone (si pensi che le posizioni creditizie attualmente attive in Italia sono diverse decine di milioni). Risultava, ad esempio, scarsamente affidabile il processo di confronto delle fotografie delineato dalla società, con un alto rischio di falsi positivi e falsi negativi, e mancava del tutto una rigorosa garanzia di affidabilità ed integrità dei dati trattati. Dagli elementi forniti all'Autorità è poi emerso che non erano state previste neppure adeguate misure di sicurezza – tra le altre, quelle a protezione della rete di comunicazione elettronica sulla quale i dati biometrici sarebbero stati trasmessi al

sistema centralizzato di acquisizione dati - con conseguenti ripercussioni per i diritti individuali in caso di violazione, di accessi di persone non autorizzate o, comunque, di abusi riguardo alle informazioni memorizzate.

Neppure la modalità di acquisizione del consenso al trattamento dei propri dati biometrici era conforme al Codice della privacy, risultando il consenso di fatto obbligato e senza che fossero previsti metodi alternativi di verifica dell'identità per accedere al finanziamento.

7. Pa e concorsi per disabili: no alle graduatorie on line
Nuovo intervento del Garante privacy. Vietata la pubblicazione di dati sanitari di centinania di persone

Stop del Garante privacy alla pubblicazione delle graduatorie di concorsi riservati ai disabili sui siti istituzionali di alcune Province e una Regione. I nominativi di centinaia di persone disabili, spesso associati a data e luogo di nascita, risultavano immediatamente visibili in rete tramite l'inserimento delle rispettive generalità nei più diffusi motori di ricerca. Nei documenti erano riportati in chiaro anche informazioni ritenute eccedenti o non pertinenti (come il reddito, la percentuale di invalidità civile, il punteggio derivante dall'anzianità, il numero di familiari a carico).

Il Garante ha dichiarato illeciti i trattamenti di dati effettuati dagli enti territoriali perché non conformi al Codice privacy che non consente la diffusione di informazioni sulla salute, tanto più on line. Oltre al provvedimento di divieto, il Garante ha prescritto alle Province interessate e alla Regione di mettersi in regola per il futuro con la pubblicazione di atti e documenti on line. Gli enti dovranno attenersi alle disposizioni della normativa e delle Linee guida in materia di trasparenza emanate dall'Autorità, adottando ogni cautela per evitare, in particolare, la diffusione di dati sanitari.

L'Autorità, inoltre, si è riservata di valutare, con separato provvedimento, gli estremi per contestare alle P.a. la violazione amministrativa prevista per l'infrazione del Codice. I casi attuali si aggiungono a numerosi episodi analoghi per i quali l'Autorità è dovuta intervenire a tutela della riservatezza vietando la pubblicazione dei dati sensibili.

A settembre dello scorso anno, il presidente del Garante per la protezione dei dati personali, Antonello Soro, ha scritto al presidente della Conferenza delle Regioni e delle Province autonome, Sergio Chiamparino, per richiamare l'attenzione della Conferenza sulla preoccupante prassi di pubblicare sui siti web degli enti pubblici atti e documenti contenenti dati personali estremamente delicati come quelli riferiti alla salute, in particolare alla disabilità.

Il Garante ha chiesto, inoltre, di valutare la possibilità di assumere specifiche iniziative affinché i trattamenti di dati effettuati da soggetti pubblici siano sempre rispettosi delle norme previste in materia di tutela della riservatezza.

8. Identità e patologie di un minore sul sito della Asl: stop del Garante Privacy

Il Garante per la privacy ha vietato* a una Asl l'ulteriore diffusione sul sito web istituzionale dei dati personali di un minore dai quali era possibile risalire alla sua identità e alle sue patologie.

L'Azienda sanitaria aveva pubblicato in internet le delibere relative alla liquidazione di fatture per l'inserimento di un minore in una comunità terapeutica riabilitativa, contenenti la descrizione dei disturbi di cui soffriva il ragazzo associati alle iniziali del suo nome e del cognome.

Nelle fatture allegate alle delibere, relative alla retta della Comunità, erano però pubblicati in chiaro e per esteso i dati anagrafici del giovane (nome, cognome, data e luogo di nascita) rendendo così identificabile il minore e causando una diffusione di dati sul suo stato di salute vietata dalle norme in materia di protezione dei dati personali. Tutte le informazioni, peraltro, erano immediatamente reperibili in rete tramite l'inserimento delle generalità del minore nei più diffusi motori di ricerca.

Ritenendo illecito il trattamento, l'Autorità ha quindi vietato alla Asl l'ulteriore diffusione in internet dei dati personali del ragazzo contenuti nelle fatture e nelle delibere.

In ottemperanza al provvedimento del Garante l'Azienda sanitaria, oltre ad anonimizzare i dati, dovrà attivarsi presso i responsabili dei principali motori di ricerca per sollecitare la rimozione della copia delle predette deliberazioni e delle fatture dagli indici e dalla cache dei motori di ricerca.

L'Asl dovrà, inoltre, per il futuro, apportare opportuni accorgimenti al fine di rendere effettivamente anonimi i dati pubblicati, oscurando i dati identificativi e tutte le altre informazioni utili ad identificare l'interessato. Le Linee guida del Garante in materia di trasparenza e pubblicità, infatti, non ritengono sufficiente, per anonimizzare i dati personali contenuti negli atti e documenti pubblicati online, la prassi di sostituire il nome e il cognome dell'interessato con le sole iniziali.

L'Autorità ha ritenuto infine di valutare con separato provvedimento gli estremi per contestare alla Asl la violazione amministrativa prevista dal Codice privacy.

9. Banche: cassette di sicurezza "self service" con le impronte digitali

Sì del Garante, ma il dato biometrico criptato deve essere solo nella smart card del cliente

Il Garante privacy ha autorizzato una banca ad installare un sistema automatizzato per la gestione delle cassette di sicurezza che consente ai clienti, attraverso l'uso delle impronte digitali, l'accesso tutti i giorni dell'anno, 24 ore su 24, senza l'intervento del personale dell'istituto di credito. Il sistema, sottoposto a verifica preliminare

dell'Autorità, non comporta la creazione di un archivio centralizzato di dati biometrici, poiché l'impronta digitale, o meglio il codice numerico (template) da essa ricavato alla prima rilevazione, è conservato esclusivamente nella smart card in possesso del cliente. Per accedere alle cassette di sicurezza il cliente deve procedere alla propria "autenticazione"mediante un codice PIN e il confronto tra la propria impronta digitale e il template memorizzato sulla smart card. A quanti, invece, non vogliono o non possono avvalersi del sistema di riconoscimento biometrico sarà comunque garantita una modalità di accesso alternativo alle cassette di sicurezza, in tal caso però fruibile solo durante l'orario di sportello e previa identificazione personale.

Nel dare il via libera al progetto, l'Autorità ha ritenuto lecito e proporzionato il trattamento di dati biometrici dei clienti, ai quali va richiesto un consenso scritto. In particolare è lecita – secondo il Garante - la finalità perseguita dalla banca di voler innalzare il livello di sicurezza e poter così coniugare la tutela dei beni conservati nelle cassette con l'utilità di garantire alla clientela un servizio continuativo. Il trattamento inoltre – sempre a parere del Garante - è risultato proporzionato, poiché non è prevista la conservazione dei dati biometrici in archivi centralizzati ma il dato criptato dell'impronta è memorizzato esclusivamente nella smart card. All'istituto di credito è stato inoltre prescritto di informare chiaramente i clienti della possibilità di un accesso alternativo alle cassette di sicurezza senza rilevazione delle impronte e di notificare all'Autorità il trattamento dei dati biometrici prima dell'inizio delle operazioni. La banca dovrà infine designare per iscritto il personale incaricato del trattamento dei dati e fornire loro adeguate istruzioni alle quali attenersi.