Per quanto riguarda gli eventi passati, il Garante ha prescritto, altresì, che qualora l'interessato ne faccia specifica richiesta, sia assicurata la conoscibilità, nel dettaglio e cronologicamente, dei dati concernenti la totalità delle variazione di punteggio della patente (provv. 24 gennaio 2013 [doc. web n. 2256617]).

4.3. LA DOCUMENTAZIONE ANAGRAFICA E LE LISTE ELETTORALI

Nel periodo di riferimento, si segnala, tra gli altri, il caso di una cittadina britannica, coniugata con un cittadino italiano, che aveva lamentato l'inesattezza di alcuni dati contenuti nell'estratto dell'atto di matrimonio. In merito è stato fatto presente che il Codice sancisce per l'interessato il diritto di accedere ai propri dati personali e fra l'altro, di ottenere "*l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati*" (art. 7, comma 3, lett. *a)*), mediante richiesta rivolta al titolare o al responsabile del trattamento dei dati personali (art. 8, comma 1, e artt. 145 e 146 del Codice) (nota 18 ottobre 2012).

In un diverso caso, un cittadino si era rivolto all'Autorità chiedendo se, ai fini dell'iscrizione nell'Anagrafe della popolazione residente e della sottoscrizione del contratto per la fornitura dell'acqua potabile di un suo inquilino, fosse legittima la richiesta avanzata dal comune di ottenere fotocopia integrale del contratto di locazione. In proposito è stato osservato che in base alla disciplina di settore l'ufficiale di anagrafe, al fine di verificare la sussistenza del requisito della dimora abituale di chi richiede l'iscrizione anagrafica, è tenuto ad effettuare gli accertamenti necessari ad appurare la verità dei fatti denunciati dagli interessati, potendo invitare gli stessi a fornire le notizie e i chiarimenti necessari alla regolare tenuta dell'Anagrafe (art. 4 l. 24 dicembre 1954, n. 1228 e art. 19 d.P.R. 30 maggio 1989, n. 223) (nota 23 agosto 2012).

Il Ministero dell'interno ha chiesto all'Autorità se, per i profili di competenza in materia di protezione dei dati personali, un consiglio notarile potesse accedere, in via telematica, "*all'archivio informatico dei cartellini delle carte di identità*" detenuto da un comune, al fine di effettuare le verifiche necessarie a contrastare furti di identità, principalmente in danno di istituti di credito. Sul punto è stato sottolineato che i comuni possono comunicare dati anagrafici anche con strumenti automatizzati e per via telematica, per finalità di snellimento

ed efficienza dell'azione amministrativa a supporto del cittadino, nel rispetto, tuttavia, degli specifici divieti di consultazione diretta degli atti anagrafici stabiliti dall'art. 37 d.P.R. n. 223/1989 (nota 29 agosto 2012). Spetta, pertanto, al comune interpellato verificare che l'accesso ai cartellini della carta di identità di cui all'art. 290 r.d. 6 maggio 1940, n. 635, avvenga in conformità ai presupposti stabiliti dalla disciplina di settore e nel rispetto delle misure di sicurezza stabilite dal Codice. Quanto all'esigenza di contrastare i furti di identità, sono state richiamate le specifiche disposizioni che prevedono in particolare che siano assoggettati a riscontro "*documenti di identità e di riconoscimento, comunque denominati o equipollenti, ancorché smarriti o rubati*" (artt. 30-*ter* e 30-*quinquies*, comma 1, lett. *a)*, d.lgs. 13 agosto 2010 n. 141, modificato dal d.lgs. 11 aprile 2011, n. 64).

Una delicata questione sottoposta all'Autorità ha riguardato la richiesta, presentata dai comuni alle strutture sanitarie presso le quali si sono verificati i parti, di riportare negli attestati di avvenuta nascita -all'atto della dichiarazione di nascita- le generalità delle puerpere che non hanno voluto riconoscere il proprio figlio (nota 25 luglio 2012). In base al quadro normativo di settore, nell'atto di nascita vanno indicate, tra le altre informazioni, le generalità dei genitori solo nei casi in cui questi ultimi "*hanno espresso con atto pubblico il proprio consenso ad essere nominati*" (artt. 29, comma 2, e 30, commi 1 e 2, d.P.R. 3 novembre 2000, n. 396) nel rispetto delle specifiche cautele previste dalle norme vigenti a tutela dell'anonimato della madre che abbia eventualmente scelto alla nascita di non voler essere nominata (v. ad es., per quanto riguarda le informazioni da riportare sul certificato di assistenza al parto, l'art. 93, comma 1, del Codice; l'art. 30, comma 1, d.P.R. n. 396/2000 e l'allegato- parte II d.m. 16 luglio 2001, n. 349). Sul punto è stata fornita ai comuni la posizione del Ministero dell'interno - Direzione centrale per i servizi demografici, il quale si è espresso nel senso di ritenere che "*L'attestazione di nascita deve contenere i dati della puerpera anche quando la medesima non intende effettuare il riconoscimento, perché il riconoscimento deve essere fatto al momento della formazione dell'atto di nascita e non può essere rimesso al momento della redazione dell'attestazione di nascita da parte dell'ostetrica o di chi ha assistito al parto. La mancanza delle generalità della puerpera, oltre a costituire un falso, si presterebbe anche ad uso illecito: se la donna non vuole riconoscere il figlio, ma il riconoscimento vuole essere fatto dall'uomo che si dichiara il*

padre, un eventuale attestazione di nascita senza il nome della puerpera consentirebbe all'uomo di presentarsi a rendere la dichiarazione di nascita, favorendo il riconoscimento da parte di altra donna che si dichiarasse madre congiuntamente all'uomo".

In relazione al rilascio delle attestazioni di stato civile, l'Autorità è intervenuta sul caso di un uomo che contestava ad un comune di aver rilasciato a un avvocato, che agiva privo di delega per conto di alcuni parenti dell'interessato, la copia integrale del suo atto di nascita, recante le informazioni sul provvedimento giudiziario riguardante la sua adozione.

L'Autorità, interpellata dal difensore civico al quale l'interessato aveva chiesto aiuto, ha però evidenziato che in base alla normativa vigente qualunque attestazione di stato civile riferita all'adottato può essere rilasciata solo con l'indicazione del nuovo cognome e con l'esclusione di qualsiasi riferimento alla paternità e alla maternità del minore (artt. 26, comma 4, e 28, comma 2, l. 4 maggio 1983, n. 184; artt. 106 e 107, commi 1 e 2, lett. *b)*, d.P.R. 3 novembre 2000, n. 396; art. 177, comma 3, del Codice), poiché indicazioni sul rapporto di adozione possano essere fornite solo su espressa autorizzazione dell'autorità giudiziaria.

Il Garante ha quindi vietato ai parenti dell'interessato l'ulteriore utilizzo delle informazioni sull'adozione contenute nella copia dell'atto di nascita. Ha poi prescritto al comune di fornire al proprio personale di stato civile adeguate istruzioni per evitare ulteriori violazioni sui dati relativi alle persone adottate. Il provvedimento è stato inoltre trasmesso all'autorità giudiziaria che potrà valutare gli eventuali illeciti penali commessi (provv. 8 novembre 2012 [doc. web n. 2187244]).

Si evidenzia ancora che un comune aveva chiesto chiarimenti in ordine alla richiesta di rilascio di copia delle liste elettorali, formulata da una società per effettuare un'indagine "*sulla rilevazione indici di ascolto e di diffusione mezzi di comunicazione*". Al riguardo, è stato evidenziato preliminarmente che il Garante si è espresso sull'argomento in varie occasioni (v. Relazione 2005 p. 65; Relazione 2006 p. 46; Relazione 2008 p. 63) specificando che le liste elettorali possono essere duplicate solo "*per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso*", secondo quanto disposto dall'art. 177, comma 5, del Codice. Spetta all'amministrazione destinataria dell'istanza di

ostensione valutare se la finalità dichiarata dal richiedente sia conforme all'attività svolta dal soggetto medesimo e se rientri effettivamente tra le ipotesi di cui al citato art. 177 del Codice. I dati personali estratti dalle liste elettorali eventualmente acquisite indebitamente non potranno essere utilizzati (art. 11, comma 2, del Codice), ferme restando le sanzioni di legge, l'adozione di ogni eventuale provvedimento inibitorio e le eventuali denunce all'autorità giudiziaria delle violazioni riscontrate (nota 25 settembre 2012).

Un ulteriore caso ha riguardato la richiesta presentata da Ancitel S.p.A. di ottenere copia delle liste elettorali in qualità di responsabile del trattamento designata da taluni enti *non profit*, che agiscono quali titolari del trattamento per finalità comprese tra quelle previste dalle vigenti disposizioni in materia (art. 51, comma 5, d.P.R. n. 223/1967, come modificato dall'art. 177, comma 5, del Codice). Nella richiesta era previsto che i predetti dati sarebbero stati successivamente trasmessi per l'elaborazione a Consodata S.p.A. anch'essa designata responsabile e da questa consegnati ai suddetti enti.

A tal proposito è stato rappresentato dall'Ufficio che le organizzazioni non lucrative, legittimate ad ottenere dai comuni il rilascio di copia delle liste elettorali e ad utilizzarle per il perseguimento delle finalità individuate dalla normativa vigente, possono richiedere a soggetti esterni (nel caso di specie Ancitel S.p.A. e Consodata S.p.A.) lo svolgimento di specifiche operazioni di trattamento. I dati, però, non possono essere comunicati ad altri titolari e possono essere utilizzati solo per le finalità perseguite dagli enti titolari del trattamento riconducibili a quelle tassativamente individuate dal citato art. 51, comma 5, del d.P.R. n. 223/1967 (nota 29 agosto 2012).

4.4. L'ISTRUZIONE

4.4.1. La scuola

Nel corso degli anni 2011 e 2012 l'Autorità ha in più occasioni fornito chiarimenti in relazione al trattamento di dati personali correlato all'istruzione pubblica.

In particolare, era stato segnalato che la ditta incaricata da una scuola pubblica di gestire il servizio di refezione scolastica inviava alle famiglie i "bollettini" non in busta chiusa, e con l'indicazione della quota spettante ad ogni bambino, consentendo così anche a soggetti non

legittimati di venire a conoscenza delle informazioni idonee a rivelare la situazione economica degli interessati. A seguito dell'intervento dell'Autorità, la predetta scuola ha garantito che i "bollettini" sarebbero stati inviati in busta chiusa sigillata (nota 7 dicembre 2011).

Con un'altra segnalazione veniva rappresentato che una scuola aveva pubblicato sul proprio sito istituzionale una circolare del dirigente scolastico indirizzata al personale docente, contenente l'indicazione dei nominativi degli alunni con specifici disturbi di apprendimento insieme ad altre informazioni relative alle loro condizioni di salute. Nell'ambito dell'istruttoria, il titolare del trattamento, nel confermare l'accaduto, ha fornito idonee assicurazioni concernenti, in particolare, l'avvenuta rimozione del documento dal web, nonché dalle copie *cache* dei principali motori di ricerca. Su tale base l'Ufficio, pur avendo riscontrato una condotta non conforme alla disciplina applicabile, non ha ritenuto sussistenti i presupposti per l'adozione di un provvedimento prescrittivo o inibitorio dell'Autorità, salva la valutazione dei presupposti per contestare la violazione del divieto di diffondere dati sensibili (art. 162, comma 2-*bis*, del Codice) (nota 9 novembre 2011).

Analogamente un istituto scolastico pubblico ha chiesto all'Autorità se l'informazione relativa alla presenza di disturbi specifici di apprendimento debba considerarsi un dato sensibile, ai sensi dell'art. 4, comma 1, lett. *d)*, del Codice.

Al riguardo, l'Ufficio ha evidenziato che i disturbi specifici di apprendimento sono considerati, dalle ricerche più accreditate, disturbi di origine neurobiologica e, in base alla normativa di settore, devono essere diagnosticati dal Servizio sanitario nazionale, sicché le relative informazioni costituiscono dati sensibili in quanto idonei a rivelare lo stato di salute degli interessati, ai sensi del Codice (art. 3, l. 8 ottobre 2010, n. 170; "Linee-guida per il diritto allo studio degli alunni e degli studenti con disturbi specifici di apprendimento" allegate al decreto del Ministro dell'istruzione dell'università e della ricerca n. 5669, del 12 luglio 2011; art. 4, comma 1, lett. *d)*, del Codice).

Tali dati devono quindi essere trattati nel rispetto delle più stringenti regole poste dal Codice per tale categorie di informazioni e della specifica normativa di settore sopra richiamata (cfr. artt. 13, 20 e 22 del Codice; regolamento adottato dal Ministero della pubblica istruzione per i trattamenti dei dati sensibili e giudiziari da effettuarsi presso il

medesimo Ministero, le istituzioni scolastiche ed educative e gli istituti regionali di ricerca educativa -si veda in particolare la scheda n. 4- d.m. 7 dicembre 2006, n. 305, sul quale il Garante ha espresso il parere di competenza in data 26 luglio 2006 [doc. web n. 1321703]) (nota 23 gennaio 2013).

La *privacy* a scuola. *Vademecum*

Prima dell'apertura dell'anno scolastico 2012-2013, l'Autorità ha pubblicato un *pamphlet,* intitolato "La *privacy* a scuola", quale contributo a favore di professori, genitori e studenti, recante alcune indicazioni generali in materia di protezione dei dati personali (6 settembre 2012 [doc. web n. 1923387]).

In tale ambito, il Garante ha precisato che possono essere assegnati temi riguardanti profili o esperienze personali affidando, qualora gli elaborati vengano letti in classe, alla sensibilità degli insegnanti la ponderazione tra esperienze didattiche e tutela della riservatezza.

Con riferimento all'uso di cellullari e *tablet* a scuola l'Autorità, nel ribadire che spetta agli istituti scolastici decidere come regolamentare l'uso di tali strumenti, ha precisato che essi possono essere utilizzati esclusivamente per fini strettamente personali (come per la ripresa e gli scatti fotografici di recite, saggi e gite scolastiche) e che non possono essere diffuse immagini, video o foto sul web se non con il consenso degli interessati.

Non possono, inoltre, essere diffusi sul sito *internet* della scuola i dati personali relativi agli studenti beneficiari di agevolazioni per il servizio di refezione scolastica ovvero dei genitori in ritardo con il pagamento della retta o del servizio di mensa. Salvi avvisi di carattere generale, le scuole devono, infatti, effettuare comunicazioni di carattere individuale per rivolgersi a singoli e specifiche persone.

Le telecamere installate all'interno delle scuole possono funzionare solo negli orari di chiusura degli istituti ed è sempre, comunque, necessario fornire un'idonea informativa sul trattamento dei dati personali effettuato tramite tali strumenti (art. 13 del Codice). Le telecamere installate all'esterno delle scuole possono, invece, riprendere solo aree strettamente pertinenti l'edificio (v. *infra* par. 4.6.).

La raccolta di informazioni personali per attività di ricerca attraverso questionari da sottoporre agli studenti è consentita solo su base volontaria, se ragazzi e genitori sono stati prima informati sugli scopi della ricerca, le modalità di trattamento e le misure di sicurezza adottate.

L'Autorità ha ribadito, inoltre, che su esplicita richiesta degli interessati e previa idonea informativa (art. 13 del Codice), le scuole e gli istituti scolastici di istruzione secondaria, per agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle predette finalità. Tali dati possono essere successivamente trattati esclusivamente a tali fini (art. 96 del Codice).

Nel ricordare il regime di pubblicità dei voti dei compiti in classe e delle interrogazioni, degli esiti degli scrutini o degli esami di Stato, i cui profili di trasparenza e conoscibilità sono comunque stabiliti dal Ministero dell'istruzione, il Garante ha precisato che è necessario che non vengano divulgate, anche indirettamente, informazioni sulle condizioni di salute degli studenti, quali il riferimento alle "prove differenziate" sostenute dai portatori di *handicap*.

L'Autorità ha anche ribadito l'obbligo per le scuole di fornire agli interessati un'idonea informativa sul trattamento dei loro dati personali e di prestare particolare attenzione alle più stringenti regole poste dal codice per il trattamento dei dati sensibili e giudiziari (artt. 20-22, 26 e 27 del Codice), ricordando a studenti e genitori i loro diritti di accesso alle informazioni che li riguardano, di rettifica e aggiornamento delle stesse (art. 7 del Codice).

L'Autorità ha, infine, auspicato che vengano previste adeguate misure di sicurezza a protezione dei dati nei provvedimenti del Ministero dell'istruzione relativi, in particolare, all'iscrizione *online* degli studenti, all'adozione dei registri *online* e alla consultazione della pagella via web, sui quali il Garante deve esprimere il proprio parere ai sensi dell'art. 154 comma 4, del Codice.

Anagrafe degli studenti

Il Garante ha formulato parere contrario, per le ragioni di seguito sintetizzate, sullo schema di Accordo tra il Ministero dell'istruzione, dell'università e della ricerca (Miur), il Ministero del lavoro e delle politiche sociali, le regioni, le Provincie autonome di Trento e Bolzano, Anci, Upi, volto a garantire l'integrazione e l'interoperabilità dell'Anagrafe nazionale degli studenti (Ans) con le Anagrafi regionali degli studenti (Ars), nell'ambito del Sistema nazionale delle anagrafi (art. 3, comma 4, d.lgs. 15 aprile 2005, n. 76).

Al riguardo l'Autorità ha individuato numerosi profili di criticità riguardanti sia i

presupposti di legittimità del trattamento dei dati personali degli studenti, sia le modalità del trattamento e la sicurezza dei dati stessi ed ha segnalato il rischio di duplicazione delle informazioni delle banche dati.

Il Garante ha in particolare evidenziato che, in via generale, sono "interoperabili" quei sistemi idonei a garantire l'intellegibilità dei dati da parte di soggetti diversi, nonché l'univocità interpretativa e la "leggibilità" del dato anche al di fuori del suo contesto iniziale.

L'Autorità ha, poi, precisato che il divieto di duplicazione di banche dati si fonda sui princìpi costitutivi della normativa in materia di protezione dei dati personali. Infatti, affinché i dati siano esatti e aggiornati è necessario, in primo luogo, prevedere l'alimentazione di un'unica banca dati, consultabile dai soggetti legittimati (art. 11 del Codice).

Ha evidenziato, inoltre, che il sistema di accessi da parte delle regioni e degli enti locali alle anagrafi del sistema non è risultato conforme alla normativa, in base alla quale le regioni e gli enti locali possono accedere all'Ans in relazione alle proprie competenze istituzionali (d.l. n. 179/2012, convertito in l. n. 221/2012). Al riguardo, il Garante ha precisato che a tal fine possono essere trattate informazioni pertinenti e non eccedenti rispetto ad una specifica funzione. I dati personali e le specifiche funzioni istituzionali per le quali tali dati sono ritenuti necessari devono, pertanto, essere preventivamente individuati in uno o più atti amministrativi attuativi della predetta norma da sottoporre al parere del Garante (artt. 11, 18, comma 2, 19, comma 1, 154, comma 1, lett. *g),* e comma 4 del Codice).

In tale quadro, l'Autorità ha inoltre rilevato che le generiche funzioni di programmazione possono essere realizzate tramite informazioni aggregate che non consentono di identificare l'interessato.

L'Autorità ha altresì rilevato, come specifica criticità inerente aspetti di legittimità, che lo schema di accordo prevedeva l'accesso da parte dell'ufficio di statistica del Ministero del lavoro e delle politiche sociali ai dati personali contenuti nell'Ans, senza adeguata previsione in tal senso della normativa di settore.

È stata inoltre evidenziata, con specifico riferimento al "gestore del sistema informativo regionale" inteso come "amministratore di sistema", la mancata conformità a quanto previsto nel provvedimento del Garante 27 novembre 2008 [doc. web n. 1577499], in quanto

all'amministratore veniva consentito di conoscere pienamente i dati contenuti nel sistema mentre, in base al citato provvedimento, le sue mansioni sono "*finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti*" senza che vi sia "*una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni)*".

Specifiche criticità sono state individuate, infine, in riferimento al sistema di codifica dei dati che avrebbe dovuto servire a garantire l'anonimato degli interessati. Il Garante ha, infatti, rilevato che la procedura di codifica, prevedendo unicamente l'attribuzione di un codice meccanografico ad ogni singolo studente, ricollegato ai dati personali dello stesso, ancorché presenti in un'altra tabella, senza specificare in particolare il criterio di accesso alla tabella di decodifica, non appariva idonea a garantire l'anonimizzazione dei dati né ad escludere che gli interessati potessero essere identificabili (parere 24 gennaio 2013 [doc. web n. 2304850]).

Diffusione sul sito web di dati personali relativi agli studenti

Nel corso dell'anno di riferimento, è stato altresì segnalato che una scuola pubblica superiore diffondeva sul proprio sito internet istituzionale l'elenco degli studenti distinti per classe. Tale diffusione, che sarebbe stata effettuata per finalità di trasparenza e pubblicità amministrativa non risultava, tuttavia, prevista da alcuna norma di legge o di regolamento (art. 19, comma 3, del Codice) (cfr. anche provv. 2 marzo 2011 [doc. web n. 1793203]).

Il Garante ha, pertanto, vietato alla scuola di diffondere ulteriormente i predetti dati personali sul proprio sito internet, salva la valutazione della sussistenza dei presupposti per contestare la violazione del divieto di diffondere dati personali in assenza di una norma di legge o di regolamento (art. 162, comma 2-*bis*, del Codice) (provv. 6 dicembre 2012 [doc. web n. 2217211]).

È stato, inoltre, segnalato che un istituto tecnico commerciale, nel diffondere sul proprio sito internet istituzionale le graduatorie relative alle supplenze del personale docente, aveva altresì consentito l'indicizzazione dei nomi degli interessati nei motori di ricerca esterni. Al riguardo, è stato evidenziato che i dati personali non devono essere liberamente reperibili utilizzando motori di ricerca esterni (cfr. art. 19, comma 3, del Codice; punto B delle citate linee-guida).

Il titolare del trattamento ha garantito di essersi conformato a tali indicazioni (nota 8 novembre 2012).

A seguito di una segnalazione, l'Ufficio ha potuto verificare che un istituto professionale aveva diffuso, sul proprio sito internet, una circolare recante l'indicazione dei nominativi degli alunni con disabilità e degli insegnanti di sostegno loro assegnati. A seguito dell'intervento dell'Ufficio l'istituto ha fornito idonee assicurazioni circa la rimozione dei predetti dati dalla rete internet.

L'Ufficio ha, tuttavia, disposto gli opportuni accertamenti per l'eventuale contestazione, con autonomo procedimento, della sanzione amministrativa di cui all'art. 162, comma 2-*bis*, del Codice per l'avvenuta violazione del divieto di diffusione dei dati sulla salute (nota 28 novembre 2012).

Flussi dati in ambito scolastico

L'Autorità è intervenuta a seguito di una comunicazione, ai sensi dell'art. 39, comma 1, lett. *a)*, del Codice, da parte di un istituto scolastico al quale un istituto superiore aveva chiesto di trasmettere dati relativi agli studenti del terzo anno della scuola secondaria di primo grado (nome, cognome indirizzo di residenza), per fornire agli stessi indicazioni relative alle nuove attività scolastiche proposte dall'istituto stesso.

Al riguardo, l'Ufficio ha ricordato, con riferimento all'attività di orientamento, che i soggetti pubblici, ivi comprese le scuole e gli istituti scolastici di istruzione secondaria possono, esclusivamente su richiesta degli interessati, comunicare e diffondere, anche per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle predette finalità (art. 96 del Codice). Ha, comunque, rappresentato che un'adeguata iniziativa di orientamento può essere svolta dai singoli istituti mettendo, ad esempio, a disposizione degli studenti presso i diversi istituti scolastici, il materiale informativo che illustri le linee distintive dei vari percorsi formativi (nota 22 gennaio 2012).

4.4.2. L'università

Nel corso dell'anno, uno studente laureato ha formulato una richiesta di chiarimenti all'Autorità sulla possibilità di ottenere, a seguito dell'avvenuta rettificazione di attribuzione

di sesso, un nuovo diploma di laurea con indicati solo i nuovi dati anagrafici. Contestualmente, l'università competente ha rappresentato al Garante la propria intenzione di rilasciare all'interessato tale secondo diploma, opportunamente evitando di dar conto del fatto che la ristampa del diploma stesso era basata su una sentenza del tribunale, di rettificazione di attribuzione di sesso, passata in giudicato.

Tale soluzione è apparsa al Garante idonea a tutelare adeguatamente la dignità degli interessati e il diritto degli stessi a vedere correttamente rappresentata la propria identità sessuale a seguito della sua modificazione. Nel medesimo provvedimento il Garante ha, altresì, prescritto a tutte le università l'adozione, nell'ambito della propria autonomia, di idonei accorgimenti e cautele affinché non siano riportate nella relativa documentazione elementi idonei a rivelare l'avvenuta rettificazione di attribuzione di sesso. Ciò fermo restando il rispetto degli obblighi di conservazione dell'atto o del documento che contiene i dati personali dell'interessato ivi compreso il sesso e il nome originario. L'Autorità ha, infine, trasmesso il predetto provvedimento al Ministero dell'istruzione, dell'università e della ricerca ed alla CRUI (Conferenza dei Rettori delle Università Italiane) per la valutazione di eventuali iniziative volte ad orientare in modo corretto e omogeneo le procedure delle università in casi analoghi (provv. 15 novembre 2012 [doc. web n. 2121695]).

Un ricercatore universitario ha rappresentato all'Autorità che un ateneo, nel pubblicare sul proprio sito gli esiti relativi alle procedure per l'assegnazione di un posto da ricercatore, aveva reso tali documenti reperibili anche in internet attraverso i più comuni motori di ricerca. Al riguardo, l'Ufficio ha ribadito che i soggetti pubblici posso diffondere dati personali, diversi da quelli sensibili e giudiziari, se ammesso da una norma di legge o di regolamento ma quando tale diffusione avviene tramite la rete internet occorre individuare specifiche garanzie atte ad impedire l'indiscriminata ed incondizionata reperibilità delle informazioni (art. 19, comma 3, del Codice; provvedimento generale del 14 giugno 2007, recante "Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" [doc. web n. 1417809]). Il titolare del trattamento ha conseguentemente fornito idonea assicurazione circa le misure assunte in conformità alle predette indicazioni del Garante (nota 12 luglio 2012).

Uno studente universitario ha segnalato all'Autorità che un ateneo aveva omesso di fornire l'informativa agli interessati e di indicare le finalità e modalità del trattamento, nonché i diritti di cui all'art. 7 del Codice (art. 13 del Codice). L'Ufficio ha quindi predisposto gli atti per l'applicazione della sanzione amministrativa (art. 161 del Codice). Con riferimento, inoltre, all'erogazione di servizi facoltativi che l'università intendeva rendere ai candidati al corso che lo studente intendeva frequentare (quali la comunicazione personale di informazioni di vario tipo, la promozione di iniziative culturali dell'università stessa o di terzi, nonché lo svolgimento di ricerche di mercato o di rilevazione del grado di soddisfazione sulla qualità dei servizi resi e sull'attività svolta dall'università), l'Ufficio ha precisato che l'ateneo è tenuto a rispettare la volontà degli interessati di beneficiarne o meno, acquisendo, di volta in volta, il loro specifico consenso al trattamento dei dati personali all'uopo necessari (nota 8 novembre 2012).

Trattamento di dati sensibili e giudiziari

La Provincia autonoma di Trento ha chiesto un parere al Garante sull'integrazione e aggiornamento del regolamento provinciale per il trattamento dei dati sensibili e giudiziari in relazione ai tipi di dati e alle operazioni eseguibili per le finalità di istruzione, educazione e formazione in ambito prescolare e scolastico e le relative finalità socio assistenziali, in ragione delle specifiche competenze attribuite dal legislatore alla Provincia stessa in materia di istruzione e formazione (artt. 68, 73, commi 1, lett. *a)* e *c)* e 2, lett. *a)* e *b)*, 86, comma 1, lett. *c)* e 95 del Codice).

In particolare, la Provincia, oltre ad aggiornare la vecchia scheda relativa all'istruzione, anche sulla base di indicazioni fornite dal Garante, ha inserito nel regolamento una nuova sezione sulle "*attività propedeutiche all'avvio dell'anno scolastico e attività educativa, didattica, formativa e di valutazione da parte delle istituzioni scolastiche e formative provinciali*", al fine di realizzare una più funzionale autonomia operativa, completando a livello provinciale, anche per il settore dell'istruzione, la disciplina del trattamento dei dati sensibili e giudiziari (parere 29 marzo 2012 [doc. web n. 1892028]).

4.5. ATTIVITÀ FISCALE E TRIBUTARIA

Sicurezza Anagrafe tributaria

Il Garante, con provvedimento del 18 settembre 2008 [doc. web n. 1549548], ha prescritto all'Agenzia delle entrate una serie di misure e accorgimenti in relazione ai livelli di

sicurezza degli accessi all'Anagrafe tributaria da parte dei soggetti esterni all'amministrazione finanziaria, prevedendo, in particolare, che l'Agenzia autorizzi i predetti accessi solo in seguito alla stipula di apposite convenzioni e che, annualmente, verifichi l'attualità delle finalità per cui ha concesso l'accesso anche con riferimento al numero di utenze attive, inibendo gli accessi effettuati al di fuori dei presupposti riconducibili all'art. 19 del Codice e quelli non conformi a quanto stabilito nelle convenzioni.

Su richiesta dell'Agenzia e dell'Anci, vista la rilevanza delle finalità istituzionali perseguite con i collegamenti all'Anagrafe tributaria da parte degli enti esterni, con il provvedimento del 16 febbraio 2011 [doc. web n. 1793806], il Garante ha prorogato il termine per tale adempimento al 15 aprile 2011, in considerazione della complessità delle attività da intraprendere, anche a fronte dell'incompleta diffusione della firma digitale presso tutti i comuni e delle difficoltà tecniche determinate dal forte afflusso di richieste pervenute sul sito dell'Agenzia per la sottoscrizione in modalità telematica della nuova convenzione.

Comunicazione integrativa annuale all'archivio dei rapporti finanziari presso l'Anagrafe tributaria

L'Agenzia delle entrate ha sottoposto al Garante lo schema di provvedimento, attuativo della recente normativa che ha introdotto nuove misure di contrasto all'evasione fiscale, riguardante le modalità con le quali le banche dovranno comunicare all'Anagrafe tributaria, per fini di controllo fiscale, le informazioni relative ai rapporti finanziari (ad es., per i conti correnti bancari, saldo iniziale e finale, importi totali degli accrediti e degli addebiti delle numerose tipologie di operazioni effettuate) (parere 17 aprile 2012 [doc. web n. 1886775]).

Tali dati, una volta raccolti, dovranno poi essere ordinati su scala nazionale per la formazione di specifiche liste di contribuenti a maggior rischio di evasione, secondo i criteri successivamente individuati con provvedimento del Direttore dell'Agenzia.

Anzitutto l'Autorità ha evidenziato che la normativa di cui lo schema è attuativo pone rilevanti problematiche relative alla protezione dei dati personali sia per l'eccezionale concentrazione presso l'Anagrafe tributaria di informazioni personali, sia in relazione alle finalità di classificazione degli interessati. Come più volte ribadito dall'Autorità -anche in sede di audizione presso la Commissione parlamentare di vigilanza sull'Anagrafe tributaria- non è, infatti, in discussione l'esigenza di disporre delle informazioni necessarie per l'azione di contrasto all'evasione fiscale, bensì l'integrale acquisizione e duplicazione presso l'Anagrafe

tributaria di una moltitudine di dati che, peraltro, genera un incremento esponenziale dei rischi e richiede misure di sicurezza di natura tecnica ed organizzativa particolarmente rigorose, sia per la trasmissione dei dati sia per la loro conservazione.

In questo quadro, in sede di istruttoria sono emerse numerose criticità relative in parte ad Entratel, il servizio telematico prescelto per la trasmissione dei dati (applicativo già in uso, oltre che per numerose comunicazioni di dati all'Anagrafe tributaria, anche per l'alimentazione dell'archivio dei rapporti finanziari), e in parte conseguenti agli aspetti tecnico-organizzativi dell'intera filiera di trattamento.

L'Agenzia ha richiesto, infatti, l'invio all'Anagrafe tributaria di una mole di dati che la gran parte degli operatori finanziari solitamente tratta con diversi sistemi applicativi, comportando quindi già all'origine una concentrazione di informazioni e, di conseguenza, un potenziale di rischio che difficilmente si riscontra nell'ordinario esercizio dell'attività benché le informazioni di base siano tutte nella disponibilità dell'operatore; infatti, solo questa specifica esigenza di conformità all'adempimento previsto dall'Agenzia rende necessaria l'aggregazione presso l'operatore medesimo, in un unico "oggetto informatico", della variegata tipologia di dati che risiederebbero altrimenti nelle diverse componenti applicative del sistema informativo.

Il Garante ha evidenziato che la scelta di utilizzare Entratel, se da un lato può semplificare l'assolvimento degli adempimenti perché già utilizzato per altre comunicazioni anche dagli operatori finanziari, dall'altro non consente di modulare le cautele rispetto alla specifica tipologia di dati che formano oggetto di ciascuna categoria di comunicazione. Entratel è risultato, infatti, inadeguato per soggetti di medio-grandi dimensioni in ragione delle voluminose quantità di scambio previste, rispetto alle potenzialità e alle limitanti caratteristiche tecniche dello strumento. Inoltre, pur rispettando le misure minime di cui all'Allegato B. al Codice, Entratel ha presentato ulteriori criticità che rendono necessario incrementarne i livelli di sicurezza per i soggetti di piccole dimensioni.

Da qui la prescrizione di dettagliate misure di sicurezza di seguito sintetizzate, da inserire nello schema di provvedimento, riguardanti sia il canale di comunicazione prescelto dall'Agenzia, sia le operazioni di trattamento dei dati finalizzate alla comunicazione delle

informazioni all'Anagrafe tributaria da parte degli operatori finanziari, volte ad assicurare, in particolare, che il procedimento di cifratura del *file* da trasmettere da parte dell'operatore finanziario possa avvenire già contestualmente alla estrazione dei dati dai sistemi, o, quantomeno, nella fase immediatamente successiva, preferibilmente con l'utilizzo di strumenti automatici.

L'Agenzia è stata pertanto invitata a predisporre l'uso di canali di comunicazione diversi e alternativi al servizio Entratel, soprattutto per le comunicazioni da parte di soggetti detentori di una elevata quantità di dati come i gruppi bancari, privilegiando l'interconnessione *application-to-application* tra i rispettivi sistemi informativi. Ciò consentirebbe di automatizzare il più possibile il processo di raccolta dei dati, rafforzando l'intera filiera di trattamento delle informazioni che, altrimenti, risulterebbero accessibili a una molteplicità di soggetti incaricati amplificando le possibilità di loro utilizzo illegittimo e migliorando la qualità dei dati trasmessi.

Invece, per l'eventuale utilizzo di Entratel, ovvero altro canale telematico, il Garante ha previsto che debbano essere introdotti da parte dell'Agenzia misure e accorgimenti volti ad assicurare innanzitutto che l'operatore finanziario possa inviare il *file*, già cifrato all'origine, in un'unica soluzione e che venga effettuata la certificazione digitale delle postazioni *client*, verificando la sicurezza delle postazioni periferiche. L'Agenzia dovrà prendere in considerazione, poi, l'utilizzo di strumenti *software* integrativi, idonei a rilevare altre qualità inerenti la sicurezza (ad es., aggiornamento dei sistemi di antivirus). Per l'autenticazione devono, inoltre, essere utilizzati sistemi di autenticazione informatica basati su tecniche di *strong authentication*, anche differenti e alternative rispetto all'utilizzo della Carta nazionale dei servizi.

Il Garante ha richiesto quindi all'Agenzia la separazione tra i profili di autorizzazione, consentendone una più completa e flessibile gestione, anche offrendo l'accesso in rete all'applicazione quantomeno su indirizzi o porte diverse da quelli utilizzabili in qualità di privato cittadino.

Per quanto attiene al trattamento posto in essere dagli operatori finanziari finalizzato alla comunicazione dei dati il Garante salva l'ipotesi dell'interconnessione *application-to-application* tra i rispettivi sistemi informativi ha disposto, in particolare, l'introduzione di meccanismi di

cifratura e di sicurezza già in fase di estrazione dei dati (finalizzati sia a proteggere le informazioni contenute nel *file* durante i successivi passaggi prima dell'invio all'Agenzia, che ad assicurare l'integrità del contenuto e a prevenirne alterazioni), la limitazione dell'accesso ai *file* ad un numero ristretto di incaricati, l'aggiornamento costante dei sistemi operativi, i *software* antivirus e antintrusione, l'eventuale conservazione dei dati solo in forma cifrata nonché, la fornitura dei *file* già cifrati ai responsabili o incaricati del trattamento.

Il Garante ha poi richiesto all'Agenzia di specificare nel provvedimento i tempi di conservazione dei dati presso l'Anagrafe tributaria e, una volta scaduti, di disporne la cancellazione automatica.

Con riferimento all'elaborazione delle liste selettive di contribuenti a maggior rischio di evasione, sulla base dei criteri successivamente individuati con provvedimento del Direttore dell'Agenzia il Garante, rilevato che l'individuazione di criteri astratti volti ad analizzare il comportamento del contribuente, soprattutto se basati sulle numerose tipologie di dati contenute in Anagrafe tributaria, presenta rischi specifici per i diritti fondamentali, la libertà, e dignità degli interessati, ha ritenuto necessario che l'Agenzia gli sottoponga il menzionato provvedimento in sede di verifica preliminare al fine di prevedere adeguate garanzie per gli interessati medesimi (artt. 14 e 17 del Codice).

Nell'ottobre 2012, l'Agenzia delle entrate ha sottoposto all'esame del Garante un nuovo schema di provvedimento volto a regolare le modalità della comunicazione integrativa annuale all'archivio dei rapporti finanziari, che ha tenuto conto delle osservazioni e delle richieste avanzate dall'Autorità, nel menzionato parere del 17 aprile 2012 [doc. web n. 1886775].

Il nuovo schema prevede che i dati vengano trasmessi attraverso una nuova infrastruttura, il "Sistema di interscambio dati" -e non più con il servizio Entratel inizialmente individuato- le cui caratteristiche, attraverso il modulo *software open Java* per il controllo formale, la compressione e la cifratura dei dati da trasmettere, consentono di automatizzare il processo di raccolta dei dati presso gli operatori finanziari, riducendo i passaggi manuali tra incaricati del trattamento che aumentano di per sé le possibilità di accessi non autorizzati e trattamenti illegittimi. Banche e operatori finanziari dovranno quindi utilizzare due modalità alternative di intercambio informatizzato con il nuovo sistema: o un *server* Ftp, cioè un "nodo" di