norma ISO/IEC 29100 per l'ambiente pubblico di cloud computing"[45]. Tali certificazioni non utilizzano la legislazione come fonte normativa, bensì si basano su altri standard tecnici. Queste possono tener conto della legislazione vigente, ad esempio nel senso che i requisiti della norma non possono essere in contraddizione con gli obblighi giuridici. Tuttavia, non viene fatto alcun riferimento diretto alla legge.

- **Certificazioni che utilizzano la legislazione come fonte per i loro criteri sostanziali**: L' ePrivacyseal UE sostiene di attestare la "conformità di un prodotto all'elenco dei criteri UE ePrivacyseal, che riflette i requisiti imposti dalla legislazione UE sulla protezione dei dati"[46]. In tal senso, tali certificazioni non promettono direttamente di offrire la conformità alla legislazione sulla protezione dei dati. Essi utilizzano tuttavia la legislazione come quadro normativo. Nell' ANNEX A sono indicati i criteri di ciascuna certificazione esistente esaminata.
- **Certificazioni che garantiscono il rispetto della legislazione**: Un esempio è il caso CNIL. L'obiettivo dei sigilli di privacy del CNIL è quello di fornire al richiedente il riconoscimento da parte dell'autorità francese per la protezione dei dati che il suo prodotto, corso, procedura "soddisfi i requisiti dell'autorità francese per la protezione dei dati" ("indicatore di fiducia")[47]. Un altro esempio del genere è EuroPrise[48]. Va osservato che l'attestazione fornita da un'autorità di protezione dei dati non deve essere interpretata erroneamente come garanzia del rispetto della legislazione, fornita dall'autorità, nel suo ruolo di controllo. Al fine di evitare tali implicazioni, la CNIL chiarisce che i sigilli CNIL per la tutela della privacy non mirano ad esentare i titolari da sanzioni amministrative pecuniarie[49]. L'ICO ha proposto un approccio diverso. Nel 2015 l'ICO ha annunciato la sua intenzione di introdurre un sigillo nazionale di riservatezza. L'obiettivo era quello di fornire un timbro per le organizzazioni che "dimostrino le buone pratiche e gli elevati standard di conformità nella protezione dei dati". L'aspetto interessante dei sigilli ICO precedentemente indicati è che il sigillo non solo dimostrerebbe la conformità ai requisiti della legge britannica sulla protezione dei dati personali, ma dimostrerebbe anche che l'organizzazione certificata supera i requisiti di legge andando "oltre il necessario".

5.8.3.1 Riferimenti normativi ed esempi di certificazione

La certificazione privacy per il GDPR viene regolamentata sulla base delle indicazioni recitate dalla norma, di seguito riassunte:

- **Considerando 100**: Deve essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano di valutare rapidamente il livello di protezione dei dati dei prodotti e servizi.
- **Articolo 42, paragrafo 1**: Incoraggia l'istituzione di meccanismi di certificazione nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al GDPR dei trattamenti.
- **Paragrafo 5**: La certificazione è rilasciata dagli OdC o dalla DPA competente in base ai criteri approvati dalla DPA o dal Board (DPB).
- **Articolo 43, paragrafo 1**: Gli organismi di certificazione sono accreditati da (opzione):
    - la DPA competente;

[45] ISO/IEC 27018:2014 "Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors", section 1 ("Scope")

[47] https://www.cnil.fr/fr/node/682

[48] Il sito web EuroPrise, ad esempio, riporta: "Certifichiamo la conformità dei prodotti IT e dei servizi basati su tecnologie dell'informazione alle normative europee sulla protezione dei dati". - https://www.european-privacy-seal.eu/EPS-en/About-EuroPriSe

[49] CNIL dichiara: "Il sigillo sulla privacy informa il pubblico che la procedura o il prodotto proposto corrisponde ai requisiti dell'Autorità per la protezione dei dati personali. A tal fine, svolge il ruolo di indicatore di fiducia. Essa non intende esonerare i suoi titolari dalle formalità amministrative." - https://www.cnil.fr/fr/questions-reponses-sur-les-labels-cnil

- dall'organismo nazionale di accreditamento (regolamento CE n. 765/2008) secondo la EN ISO/IEC 17065:2012 (relativa ai prodotti[50], processi[51] e servizi[52]) e i requisiti aggiuntivi stabiliti dalla DPA competente.

Questa viene citata anche:

- **nell'Articolo 24 paragrafo 3**: L'adesione ai codici di condotta o al meccanismo di certificazione può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.
- **nell'Articolo 25 paragrafo 3**: Il meccanismo di certificazione può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 [attuare in modo efficace i principi di protezione dei dati] e 2 [trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento] del presente articolo.
- **nell'Articolo 28 paragrafo 5**: L'adesione da parte del responsabile del trattamento a un codice al meccanismo di certificazione può essere utilizzata come elemento per dimostrare le garanzie sufficienti.
- **nell'Articolo 32 paragrafo 3**: L'adesione a un codice di condotta o al meccanismo di certificazione può essere utilizzata come elemento per dimostrare di garantire un livello di sicurezza adeguato al rischio.

Ma ci si riferisce anche ai codici di condotta, come ad esempio:

- **nell'Articolo 40**: Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta.
- **nell'Articolo 41 (paragrafo 1)**: il controllo della conformità con un codice di condotta ai sensi dell'articolo 40 può essere effettuato da un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'autorità di controllo competente.
- **nell'Articolo 41 (paragrafo 3)**: L'autorità di controllo competente presenta al comitato il progetto di requisiti per l'accreditamento dell'organismo.
- **nell'Articolo 41 (paragrafo 4)**: un organismo adotta le opportune misure in caso di violazione del codice da parte di un titolare del trattamento o responsabile del trattamento. Esso informa l'autorità di controllo competente di tali misure e dei motivi della loro adozione.

Relativamente alla certificazione delle persone, si può dire che, la posizione più comune è che gli articoli del GDPR relativi alla certificazione non includono le persone. In Spagna è stato pubblicato nel Luglio del 2017 uno schema relativo al profilo del DPO, mentre in Italia, da tempo, si sta lavorando (in attesa di prossima pubblicazione) su una norma "Profili professionali relativi al trattamento e alla protezione dei dati personali".
La certificazione regolamentata coinvolge i seguenti attori:

- gli enti di normazione (quelli ufficiali sono regolamentati dal Regolamento Europeo 1025/2012) che emettono norme, e possono essere:
  - enti nazionali (UNI e UNINFO, BSI, DIN, etc.);
  - enti internazionali (CEN/CENELEC, ISO, IEC);
  - enti privati.

50 Risultato di un processo; servizi (per esempio, trasporto), software (per esempio, un programma per computer, il contenuto di un vocabolario), hardware (per esempio, la parte meccanica di un motore), materiali da processo continuo (per esempio, un lubrificante).

51 Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita; esempi sono i processi di tratamento termico, di fabbricazione, di produzione di cibo, di crescita di un impianto.

52 Risultato di almeno un'attività necessariamente effettuata all'interfaccia tra il fornitore e il cliente, che è generalmente intangibile; esempi sono: riparazione di un'automobile, elaborazione della dichiarazione dei redditi, erogazione di formazione, messa a disposizione di una camera d'albergo.

- Gli organismi di accreditamento sorvegliano le attività di certificazione, accreditando (e verificando) gli organismi di certificazione. Questi si riconoscono mutualmente tra di loro (MLA), e in Europa, rispondono al Regolamento europeo 765/2008. Tali organismi operano secondo standard definiti come ISO/IEC 17011 e recepiscono anche altre norme.
- Gli organismi di certificazione, certificano le organizzazioni o i prodotti, processi e servizi, e selezionano gli auditor. Questi lavorano secondo standard definiti (ISO/IEC 17021, 17065, ecc.) e certificano organizzazioni e persone secondo "specifiche".
- Le organizzazioni e le persone che si vogliono certificare. La certificazione deve avvenire nel rispetto di norme specifiche (es. ISO 9001, UNI 11506, ecc.) dove tali specifiche possono essere pubblicate da chiunque.

E' necessario stabilire una regolamentazione degli organismi di certificazione in merito:

- alla modalità di conduzione degli audit;
- alle verifiche sulla conduzione degli audit;
- al mantenimento dei certificati (sorveglianza, verifiche in occasione di modifiche);
- alla gestione dei reclami;
- alla trasparenza e all'imparzialità;
- alle competenze del personale.

Gli Enti di accreditamento (soprattutto in Italia) pubblicano requisiti aggiuntivi a quelli delle norme ISO per gli OdC. Gli Organismi di certificazione devono pubblicare un regolamento relativo alle attività di certificazione dei prodotti, processi e servizi. Il regolamento dettaglia alcuni processi generali (per esempio la gestione dei reclami dei clienti) e dettaglia come svolgere gli audit in termini di:

- numero e tipo di verifiche di certificazione, sorveglianza e ri-certificazione;
- modalità di condivisione del rapporto;
- tipo di rilievi (classificazione delle non conformità) e loro gestione (per esempio, a fronte di non conformità gravi è necessario un audit straordinario entro poche settimane).

Dal punto di vista del funzionamento della certificazione è possibile prevedere un "sistema di certificazione alternativo" dove l'ente di accreditamento non ha accordi con altri enti, e in Europa, non risponde al Regolamento CE n. 765/2008 (ossia in competizione con l'ente nazionale), nel contempo, l'OdC non è accreditato e eroga alcuni servizi non accreditati e le specifiche vengono scritte da enti non "pubblici" o non riconosciuti. In alcuni casi, le attività non accreditate hanno come obiettivo di promuovere un sistema "normato" (in altre parole, fungono da prototipi), in altri invece, le attività non accreditate hanno come finalità la creazione di un mercato "parallelo" (pertanto non apprezzato da chi promuove il mercato "normato").
La sicurezza delle informazioni si basa sulla buona gestione, ovvero sulla giusta scelta di buoni processi di selezione, attuazione e manutenzione che portano a loro volta ad una buona scelta tecnologica. In tal senso, le normative note sono:

- Sistemi di gestione noti e diffusi:
  - ISO 9001:2015 per la qualità;
  - ISO/IEC 27001:2013 per la sicurezza delle informazioni.
- Sistemi di gestione per la privacy (standard nazionali):
  - BS 10012:2017 (UK);
  - JIS 15001:2006 (JP);
  - ISO/IEC 29151 (estensione della ISO/IEC 27001 solo per i titolari);
  - ISO/IEC 27018 (estensione della ISO/IEC 27001 solo per i fornitori di cloud pubblici);
  - ISO/IEC 27552 (di sistema di gestione, estensione della ISO/IEC 27001, disponibile da Agosto 2019).

Le certificazioni dei sistemi di gestione sono governate dalla ISO/IEC 17021, ma il GDPR cita la ISO/IEC 17065.
Dal considerando 100 del GDPR, si deduce che un trattamento è riconducibile ad un servizio e come tale si riportano a titolo puramente indicativo, alcuni esempi di certificazione:

- Centri di contatto multicanale (norme EN 15838:2010 e UNI 11200:2010)
  - Regolamento Accredia RT-22;
  - la EN 15838 include il ciclo PDCA (strategia, attività operative, riesami periodici, gestione del miglioramento);
- Erogazione di corsi di formazione;
- Vigilanza (norma UNI 10891);
- Centri di monitoraggio e ricezione allarmi (EN 50518 e UNI 11068);
- Fornitori di servizi eIDAS;
  - I requisiti consigliano l'adozione della ISO/IEC 27001;
- Fornitori di servizi SPID (richiesta la certificazione ISO/IEC 27001).

In modo analogo, si riportano a seguire alcuni esempi di certificazione di prodotto:

- Attualmente "lo" schema di certificazione della sicurezza dei prodotti informatici è costituito dalla ISO/IEC 15408 (Common Criteria);
  - richiede l'attuazione di processi molto simili (e forse più rigorosi) di quelli richiesti dai sistemi di gestione per la qualità.
- Gli schemi di certificazione di prodotto sono tanti, tra cui:
  - Regolamento Reg. CE 303/2008 (apparecchiature con gas fluorurati);
  - Direttiva PED (per i recipienti in pressione);
  - Direttiva MED (dispositivi medici).
- In molti casi è richiesto un sistema di gestione (per la qualità), anche se non necessariamente certificato.

In tale ambito esistono delle iniziative italiane, quali:

- L'11 settembre del 2018 è entrata in vigore la "Prassi di riferimento UNI" dal titolo "Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento europeo EU 679/2016 (GDPR)" che ha le seguenti caratteristiche:
  - non è uno standard di requisiti certificabili;
  - è solo per l'ICT (comunque molto importante);
  - è comunque un punto di riferimento.
- Sulla base di bozze della norma "Profili professionali relativi al trattamento a alla protezione dei dati personali" di prossima pubblicazione, che riguarda il DPO, il Manager privacy, lo Specialista privacy e il Valutatore privacy, alcuni registri stanno promuovendo schemi di certificazione professionali.

Per il futuro, non risultano allo studio delle DPA degli schemi condivisi per i servizi. Esiste un interesse sulla ISO/IEC 27552. Alcuni Enti promuovono schemi "proprietari" non promossi da alcuna DPA (non secondo criteri approvati da alcuna DPA). Il comunicato emesso dal Garante Privacy e Accredia del 18 luglio 2017 riporta quanto segue: *in Italia non è ancora stato stabilito dal Legislatore nazionale a chi spetti il ruolo di ente di accreditamento ai fini del regolamento, né sono stati definiti i "requisiti aggiuntivi" per l'accreditamento degli organismi di certificazione (cfr. art. 43, paragrafo 1, lettera b) e i criteri di certificazione (cfr. art. 42 paragrafo 5)*. Esistono schemi promossi solo da una DPA (con valore reale solo in un Paese – Label CNIL, dal 2011; 12 label Gouvernance e 1 label relativa ai servizi) e schemi promossi da EuroPriSe (dal 2008, meno di 50 "seals" per prodotti, servizi e siti web) e ePrivacy Seal (dal 2011, circa 200 "seals" per prodotti). Gli schemi per la certificazione di prodotti, solitamente sono molto complessi da realizzare in ambito IT e molto onerosi da certificare. Forse alcuni schemi nazionali (o europeo), meno onerosi dei Common Criteria, si imporranno sul mercato europeo generale.