cloud in base al grado di soddisfazione dei meccanismi di sicurezza e privacy ottenuti dai potenziali fornitori cloud. Sebbene si tratti di un framework che fornisce procedure dettagliate per analizzare i requisiti di sicurezza e privacy, non è disponibile alcuna conoscenza reale della sicurezza e della privacy.
Riferimento bibliografico: Haralambos Mouratidis, Shareeful Islam, Christos Kalloniatis, and Stefanos Gritzalis. A framework to support selection of cloud providers based on security and privacy requirements. Journal of Systems and Software, pages 2276–2293, 2013.

5.8.6.7 Adaptive privacy

Omoronyia et al. [9] propone un framework di riferimento per supportare la divulgazione selettiva delle informazioni personali da parte di applicazioni software in un contesto in continuo cambiamento. Il framework si concentra sui requisiti di sensibilizzazione alla privacy (PAR - privacy awareness requirements) e descrive:

1. come identificare gli attributi da monitorare per rilevare le minacce alla privacy,
2. come scoprire le minacce alla privacy prima della divulgazione delle informazioni personali,
3. come determinare la gravità, così come i benefici relativi a una minaccia scoperta.

Il quadro normativo richiede tuttavia che i requisiti di riservatezza di tutti gli agenti siano già definiti e non fornisce indicazioni su come ottenerli.
Riferimento bibliografico: Inah Omoronyia, Luca Cavallaro, Mazeiar Salehie, Liliana Pasquale, and Bashar Nuseibeh. Engineering adaptive privacy: on the role of privacy awareness requirements. In Proceedings of the 2013 International Conference on Software Engineering, ICSE ’13, pages 632–641. IEEE Press, 2013.

5.8.6.8 STRAP

STRAP [10] è un framework di analisi della privacy che è stato sviluppato sulla base dei risultati dell'analisi di sei framework esistenti (modelli di rischio [16], Patrick e Kenny [17], framework i* [18], Langheinrich [19], Bellotti e Sellen [20], e valutazione euristica [21]). Si tratta di un metodo a cinque fasi, che consiste in una analisi orientata agli obiettivi, analisi della vulnerabilità, perfezionamento e progettazione degli obiettivi, valutazione del progetto e iterazione. La fase di analisi della vulnerabilità è la fase principale in cui vengono combinati i framework esistenti. L'analisi si basa su una serie di domande analitiche per determinare la cattura e l'uso delle informazioni. In secondo luogo, viene utilizzata l'euristica per identificare potenziali problemi basati su difetti e requisiti comuni. Queste euristiche possono essere classificate secondo le FIPP degli Stati Uniti: notice/awareness, choice/consent, integrity/security, enforcement/redress. Sebbene queste categorie, basate sulla legislazione e sugli orientamenti in materia di protezione dei dati, siano molto importanti dal punto di vista della tutela della privacy, non tengono conto delle proprietà fondamentali quali l'anonimato, la non collegabilità e la non rilevabilità.
Riferimento bibliografico: Carlos Jensen. Designing for privacy in interactive systems. PhD thesis, Georgia Institute of Technology, 2005.

5.8.6.9 Microsoft privacy guidelines

Le linee guida sulla privacy fornite da Microsoft descrivono alcuni concetti basilari di privacy [11], come diversi tipi di consenso o concetti di minimizzazione dei dati. Inoltre, per gli scenari selezionati vengono presentate alcune linee guida riguardanti i seguenti principi: avviso, scelta, trasferimento successivo, accesso, sicurezza e integrità dei dati. Tuttavia, contiene solo un elenco piatto degli orientamenti richiesti e raccomandati e non intende descrivere un approccio più strutturato. Queste linee guida possono essere utilizzate come ispirazione per determinare le possibili minacce, ad esempio per ampliare il catalogo degli alberi delle minacce.