- individuare gli obiettivi di tutela della privacy,
- analizzare l' impatto degli obiettivi di tutela della privacy sui processi organizzativi,
- modellare i processi interessati utilizzando modelli di tutela della privacy
- identificare le tecniche che meglio supportano o implementano i processi summenzionati.

Riferimento bibliografico: Christos Kalloniatis, Evangelia Kavakli, and Stefanos Gritzalis. Addressing privacy requirements in system design: the PriS method. Requirements Engineering, 13(3):241–255, 2008.

5.8.6.4 FPFSD

Spiekermann e Cranor [6] hanno sviluppato un framework denominato (FPFSD). Questo è un framework per la progettazione di sistemi rispettosi della privacy (framework for privacy-friendly system design) in cui si attua una distinzione tra due diversi approcci alla privacy:

- Privacy-by-policy, introduce l'approccio di notifica e consenso basato sui principi di Fair Information Practice Principles (FIPP) e implica che l'utente sia informato su quali informazioni vengono utilizzate e perché. Inoltre, l'utente può decidere di non fornire dati.
- Privacy-by-architecture, incoraggia l'archiviazione dei dati presso il cliente invece di far archiviare le informazioni riservate dalle aziende stesse.

Riferimento bibliografico: Sarah Spiekermann and Lorrie F. Cranor. Engineering privacy. IEEE Transactions on Software Engineering, 35(1):67–82, 2009.

5.8.6.5 MPRA

Gürses [7] propone una tecnica multilaterale per l'analisi dei requisiti in materia di tutela della privacy (multilateral privacy requirements analysis technique). Si articola in tre fasi principali: analisi degli stakeholder, analisi funzionale e analisi della privacy. In primo luogo vengono determinati gli attori e le parti interessate. Per ciascuno di questi, vengono determinati gli obiettivi funzionali che vengono poi collegati alle ipotesi di dominio. Viene inoltre creato un modello informativo. Nella fase finale, le problematiche sulla privacy sono determinate in base a ciascun stakeholder, in relazione al modello informativo e agli obiettivi funzionali individuati nella fase precedente. Tali problematiche possono anche tradursi in minacce alla privacy e documentate come casi di abuso. Infine, le problematiche (o minacce) vengono trasformate in obiettivi di tutela privacy come un'approssimazione giustificabile.
Riferimento bibliografico: Fahriye Seda Gürses. Multilateral privacy requirements analysis in online social network services. PhD thesis, Department of Computer Science, KU Leuven, 2010.

5.8.6.6 Privacy in the Cloud

Mouratidis et al. [8] pone in particolare l'attenzione sulle applicazioni cloud proponendo un framework che supporta l'elicitazione dei requisiti di sicurezza e privacy. Il framework è composto da un linguaggio (basato su Secure Tropos[56]) e da un processo (basato su PriS) a supporto dell'analisi della sicurezza e della privacy. Il processo si articola in tre fasi. Il primo passo (facoltativo) è la catalogazione delle minacce alla sicurezza e alla privacy, che mira a creare un punto di riferimento basato sull'esperienza passata da utilizzare poi successivamente. In secondo luogo, l'attività di analisi della sicurezza e della privacy consiste in due sotto-attività: la definizione del contesto organizzativo, in cui vengono identificati gli obiettivi organizzativi, gli attori e le dipendenze, i piani e le risorse e gli obiettivi di sicurezza e privacy; e la definizione delle possibili problematiche in materia di sicurezza e privacy, che consiste nell'identificare i requisiti, le misure e i meccanismi di sicurezza e privacy. Il terzo e ultimo passo è la selezione del provider dei servizi

[56] http://www.troposproject.eu/node/301