	Privacy preserving biometrics	**X**	**X**			**X**		
Encryption techniques	Symmetric key & public key encryption					**X**		
	Deniable encryption			**X**		**X**		
	Homomorphic encryption					**X**		
	Verifiable encryption					**X**		
Access control techniques	Context-based access control					**X**		
	Privacy-aware access control					**X**		
Policy and feedback tools	Policy communication (P3P)							**X**
	Policy enforcement (XACML, EPAL)							**X**
	Feedback tools for user privacy awareness						**X**	
	Data removal tools (spyware removal, browser cleaning tools, activity traces eraser, harddisk data eraser)						**X**	

Tabella 27 - Mappatura tra obiettivi e tecniche di miglioramento della privacy

* **U**–Unlinkability, **A**–Anonymity/Pseudonymity, **P**–Plausible deniability, **D**–Undetectability/unobservability, **C**–Confidentiality, **W**–Content Awareness, **O**–Policy and consent compliance of the system

5.8.6.2 PRoPAN

Beckers et al. [4] ha creato un approccio in quattro fasi per l'identificazione semiautomatica delle minacce alla privacy. Il metodo ProPAn (Problem-based Privacy Analysis) contribuisce nella produzione dei requisiti di protezione della privacy ed è un approccio basato su problemi per l'identificazione semiautomatica delle minacce alla privacy durante l'analisi dei requisiti dei sistemi software. L'obiettivo di questa metodologia è quello di assistere gli ingegneri del software nella requisitazione al fine di ottenere le seguenti informazioni:

- conoscenza del settore rilevante per la privacy;
- dati personali trattati;
- requisiti di riservatezza.

La metodologia consiste in quattro fasi:

- Disegno del diagramma di contesto e dei diagrammi dei problemi,
- Aggiunta dei requisiti di privacy al modello,
- Generazione di grafici delle minacce alla privacy,
- Analisi dei grafici delle minacce alla privacy.

Riferimento bibliografico: Kristian Beckers, Stephan Faßbender, Maritta Heisel, and Rene Meis. A Problem-based Approach for Computer Aided Privacy Threat Identification. In Privacy Technologies and Policy, volume 8319 of LNCS, pages 1–16. Springer, 2014.

5.8.6.3 PriS

PriS [5] è un metodo di ingegnerizzazione dei requisiti di sicurezza, che integra i requisiti di riservatezza già nelle fasi iniziali del processo di sviluppo del sistema. PriS considera i requisiti relativi alla privacy come obiettivi organizzativi che devono essere soddisfatti e adotta l'uso di modelli di processi di privacy come un modo per:

1. descrivere l'effetto dei requisiti relativi alla privacy sui processi aziendali;
2. facilitare l'identificazione dell'architettura di sistema che meglio supporta i processi aziendali in relazione agli aspetti di privacy.

In questo modo, PriS fornisce un approccio olistico che va dagli obiettivi di alto livello ai sistemi informatici "rispettosi della privacy". Il metodo si articola in quattro fasi: