Identifiability of (E,DF)	Anonymity/pseudonymity of (E,DF)
Identifiability of (E,DS)	Anonymity/pseudonymity of (E,DS)
Identifiability of (E,P)	Anonymity/pseudonymity of (E,P)
Non-repudiation of (E,DF)	Plausibledeniability of (E,DF)
Non-repudiation of (E,DS)	Plausibledeniability of (E,DS)
Non-repudiation of (E,P)	Plausibledeniability of (E,P)
Detectability of DF	Undetectability of DF
Detectability of DS	Undetectability of DS
Detectability of P	Undetectability of P
Information Disclosure of DF	Confidentiality of DF
Information Disclosure of DS	Confidentiality of DS
Information Disclosure of P	Confidentiality of P
Content Unawareness of E	Content awareness of E
Policy and consent Noncompliance of the system	Policy and consent compliance of the system

Tabella 25 - obiettivi di privacy basati sule varie tipologie di minaccia previste in LINDDDUN

5.8.6.1.1 Tecniche di mitigazione

Nella metodologia LINDDUN, le proprietà e la corrispettive minacce alla privacy vengono classificate come hard e soft privacy. La tabella a seguire evidenzia tale classificazione:

Proprietà di privacy	Minaccia alla privacy
Hard privacy	
Unlinkability	Linkability
Anonymity & Pseudonymity	Indentifiability
Plausible deniability	Non repudiation
Undetectability & unobservability	Detectability
Confidentiality	Disclosure of information
Soft privacy	
Content awareness	Content Unawareness
Policy and consent compliance	Policy and consent non-compliance

Tabella 26 - LINDDUN Hard & Soft privacy

LINDDUN fornisce per ogni tipo di potenziale minaccia identificata una o più classificazioni delle tecniche di mitigazione da mettere in campo attraverso una mappatura tra obiettivi e tecniche di miglioramento della privacy (PETs):

	Tecniche di mitigazione	U	A	P	D	C	W	O
Anonymity system	• Mix-networks (1981) • DC-networks (1985) • ISDN-mixes • Onion Routing (1996) • Crowds (1998) • Single proxy (90s) (Penet pseudonymous remailer (1993-1996), Anonymizer, SafeWeb) • Anonymous Remailer (Cipherpunk Type 0, Type 1, Mixmaster Type 2 (1994), Mixminion Type 3 (2003)) • Low-latency communication (Freedom Network (1999-2001), Java Anon Proxy (JAP) (2000), Tor (2004))	X	X			X		
	• DC-net & MIX-net + dummy traffic • ISDN-mixes	X	X		X	X		
	• Broadcast systems + dummy traffic	X	X		X			
Privacy preserving authentication	• Private authentication • Anonymous credentials (single show, multi show)	X	X					
	• Deniable authentication	X	X	X				
	• Off-the-record messaging	X	X	X		X		
Privacy preserving cryptographic protocols	Multi-party computation (Secure function evaluation)	X				X		
	Anonymous buyer-seller watermarking protocol	X	X			X		
Information retrieval	Private information retrieval + dummy traffic	X	X		X			
	Oblivious transfer	X	X			X		
	Privacy preserving data mining	X	X			X		
	• Searchable encryption • Private search		X			X		
Data anonymization	• K-anonymity model • l-Diversity	X	X					
Information hiding	Steganography	X	X		X			
	Covert communication	X	X		X			
	Spread spectrum	X	X		X			
Pseudonymity systems	Privacy enhancing identity management system	X	X					
	User-controlled identity management system	X	X					