- Ripudio (Plausible Deniability);
- Non rilevabilità (Undetectability);
- Non divulgazione di informazioni (Confidentiality);
- Consapevolezza sul contenuto (Content Awareness);
- Aderenza alla politica sul consenso (Policy and consent compliance).

LINDDUN viene presentato come un approccio completo alla modellazione delle minacce con un metodo di individuazione di processi, minacce e requisiti. Può essere ragionevole utilizzare LINDDDUN come framework per l'identificazione delle minacce sulla privacy, in sostituzione o in aggiunta alla STRIDE.
In primo luogo, viene creato un diagramma di flusso dei dati (DFD), una rappresentazione grafica strutturata del sistema che utilizza quattro tipi principali di elementi: entità, archivi dati, flussi di dati e processi. Ciascun tipo di elemento DFD viene associato a una serie di categorie di minacce alla privacy (sono state identificate sette categorie di alto livello di minacce alla privacy: **L**-Linkability, **I**-Identifiability, **N**-Non Repudiation, **D**-Detectability, **D**-Disclosure of information, **U**-Content Unawareness e **N**-Policy and consent Non-compliance). Per identificare le minacce che insistono sul sistema analizzato, per ciascun elemento è necessario esaminare le minacce corrispondenti alle categorie di cui sopra.
La tabella seguente, mostra la correlazione tra le minacce di privacy previste da LINDDUN e le tipologie di elementi DFD sopra descritte:

Elemento DFD	L	I	N	D	D	U	N
Archivio dati	X	X	X	X	X		X
Flusso dati	X	X	X	X	X		X
Processo	X	X	X	X	X		X
Entità	X	X				X	

Tabella 24 - Minacce LINDDUN per elemento DFD

La metodologia LINDDUN supporta l'analista fornendo una serie di alberi di minaccia che descrivono i percorsi d'attacco più comuni per ogni possibile combinazione tra le tipologie di minaccia e gli elementi DFD. Basandosi su questi alberi, l'analista potrà documentare le minacce identificate, utilizzando scenari di casi di abuso per descrivere in dettaglio i possibili attacchi. Le minacce vengono quindi considerate prioritarie in base al loro rischio. Tuttavia non fornisce esplicitamente un supporto per l'analisi del rischio. Le minacce che derivano da tale processo, possono quindi essere tradotte in requisiti di riservatezza. Infine, LINDDUN fornisce un elenco di soluzioni per la privacy al fine di mitigare le minacce individuate.

La tabella seguente, riporta gli obiettivi di privacy (proprietà della privacy) basati sule varie tipologie di minaccia previste in LINDDUN, dove (**E**-Entità, **DF**-Flusso Dati, **DS**-DataStore, **P**-Processo).

Minacce LINDDUN	Obiettivo elementare a tutela della privacy
Linkability of (E,E)	Unlinkability of (E,E)
Linkability of (DF,DF)	Unlinkability of (DF,DF)
Linkability of (DS,DS)	Unlinkability of (DS,DS)
Linkability of (P,P)	Unlinkability of (P,P)
Identifiability of (E,E)	Anonymity/pseudonymity of (E,E)