4. è largamente impiegata (ad es. OWASP[59] e OpenStack[60]) .

6.5 Modellazione e Individuazione delle minacce di privacy con LINDUN

La privacy è un aspetto molto importante, soprattutto nella società odierna, dove i dati personali sono onnipresenti e purtroppo questa, viene spesso trascurata durante lo sviluppo del software. Nonostante emergono diverse metodologie orientate alla produzione di requisiti di tutela della privacy (vedi paragrafo 5.8.6), queste non soddisfano appieno quelle che sono le aspettative, o comunque, non sono in grado di fornire una guida metodologica sostanziale da adottare nel corso dell'analisi o mancano del necessario supporto alla tutela della privacy.
Per colmare questa lacuna, si propone la metodologia LINDDUN, descritta nei capitoli precedenti. LINDDUN si ispira infatti a STRIDE, ovvero, un approccio consolidato per la modellazione e l'identificazione delle minacce alla sicurezza. Inoltre, la metodologia LINDDUN è stata costruita sulla base delle classificazioni esistenti in materia di tutela della privacy.
Anche se LINDDUN non è una tecnica di conformità, attua diversi principi imposti dalla legislazione sulla protezione dei dati (ad esempio consenso, minimizzazione, sensibilizzazione, ecc.) e richiama esplicitamente l'attenzione sulla necessità di conformità normativa. Inoltre, le proprietà sulla privacy, riportate nel paragrafo 5.8.1.1, costituiscono la base delle categorie di minacce gestite da LINDDUN. Infine, LINDDUN aderisce anche ai principi della Privacy by Design in quanto mira a introdurre la privacy nelle prime fasi del ciclo di vita di sviluppo del software.

[59] https://www.owasp.org/index.php/Threat_Risk_Modeling

[60] https://wiki.openstack.org/wiki/Security/OSSA-Metrics#DREAD