due fattori. Se ciò non è possibile, permettere agli utenti di creare e personalizzare le proprie domande mettendoli in guardia contro la scelta di domande che contengono dati personali. Tutte le informazioni fornite devono essere cifrate.

- **Creare termini e condizioni chiari e assicurarsi che gli utenti li leggano**: Non nascondere i termini e le condizioni. In base alle nuove leggi dell'UE sulla privacy, i termini e le condizioni devono essere presenti sulla pagina iniziale di qualsiasi applicazione ed essere altamente visibili durante la navigazione dell'applicazione da parte dell'utente. È necessario implementare un meccanismo nell'applicazione tale per cui gli utenti debbano accettare i termini e le condizioni prima di poter accedere all'applicazione stessa, e in particolar modo, quando tali termini sono stati oggetto di modifica. I termini e le condizioni devono inoltre essere redatti in un linguaggio facilmente comprensibile dall'utente finale.
- **Informare gli utenti di qualsiasi condivisione dei loro dati con terze parti**: Se l'organizzazione ha la necessità di condivide i dati personali degli utenti con terze parti, siano essi componenti software esterni, affiliati o organizzazioni governative, ciò deve essere esplicitato nei termini e condizioni.
- **Creare dei criteri chiari per le violazioni dei dati personali**: Uno degli aspetti più importanti della legge dell'UE è il diritto degli utenti di essere informati in caso di violazione dei propri dati. Le organizzazioni devono implementare politiche chiare che stabiliscano ruoli e procedure da seguire in modo tale che, ad esempio, questi vengano tempestivamente informati a fronte di ogni violazione.
- **Rimuovere i dati personali degli utenti quando questi annullano la propria sottoscrizione al servizio**: Molte applicazioni non forniscono con chiarezza informazioni riguardo il trattamento dei dati personali relativi ad un utente che ha annullato la propria sottoscrizione al servizio o che ha cancellato il proprio account. Con il diritto di essere dimenticati, le organizzazioni devono rispettare il diritto degli utenti di cancellare il proprio account e tutti i relativi dati associati. Deve essere chiaro e visibile a tutti gli utenti che possono abbandonare il servizio e che sistematicamente tutti i loro dati verranno cancellati. Le organizzazioni che trattano gli account cancellati semplicemente come inattivi, potrebbero essere in contrasto con la normativa.
- **Patch delle vulnerabilità del Web**: Come menzionato nell' elenco OWASP Top 10[54], uno dei principali rischi per la privacy dei dati riguarda le vulnerabilità delle applicazioni web: "La vulnerabilità è un problema chiave in qualsiasi sistema che protegga o operi su dati sensibili dell'utente. La progettazione e l'implementazione inadeguata di una applicazione, la rilevazione di un problema o l'applicazione tempestiva di una correzione (patch) possono comportare una violazione della privacy. Assicurarsi che l'organizzazione disponga di un programma capace di valutare i rischi informatici ed eseguire efficacemente test di penetrazione e patch.

5.8.6 Tecniche di modellazione e individuazione delle minacce

5.8.6.1 LINDDUN

La privacy è diventata una questione chiave nell'e-society. È della massima importanza che la privacy sia integrata quanto prima nel ciclo di vita del software di sviluppo. LINDDUN[55] è una metodologia di analisi delle minacce alla privacy e supporta gli analisti nell'individuare i requisiti di riservatezza.
LINDDUN è un nome mnemonico sviluppato da Mina Deng [15] per il suo dottorato di ricerca alla Katholieke Universiteit di Leuven, Belgio. Questa è una metodologia speculare alla modellazione delle minacce STRIDE (STRIDE-per-element) e tratta le violazioni delle seguenti proprietà sulla privacy:

- Non collegabilità (Unlinkability);
- Non identificabilità (Anonymity/Pseudonymity);

54 https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project

55 https://www.linddun.org/