sistema (comprendente questi ed eventualmente altri elementi), l'aggressore non sia in grado di identificare in modo efficace se tali IOI sono o meno tra loro collegati.

- **Anonymity**. Si riferisce alla capacità di nascondere il legame tra un'identità e un'azione o un'informazione (ad esempio, il mittente anonimo di una e-mail, l'autore di un testo, la persona che accede ad un servizio, la persona a cui si riferisce una voce presente in un database). Tale proprietà assicura che un eventuale attaccante non possa identificare in modo efficace il soggetto. L'anonimato può essere ricondotto anche alla precedente proprietà (unlinkability).
- **Pseudonymity**. Suggerisce che è possibile costruire una reputazione su uno pseudonimo e utilizzare pseudonimi multipli per scopi diversi.
- **Plausible deniability**. Si riferisce alla capacità di ostacolare la possibilità da parte di un attaccante di dimostrare che un soggetto conosce, ha fatto o ha detto qualcosa.
- **Undetectability and unobservability**. Si riferisce alla capacità di nascondere le attività dell'utente. L'*undetectability* è vista come l'impossibilità di rilevare un elemento di interesse (IOI) da un punto di vista di un attaccante, il che significa che quest'ultimo non può distinguere quando l'elemento esiste da quando invece non esiste. L'*unobservability* è vista come l'impossibilità di osservare un elemento di interesse (IOI) da parte di tutti i soggetti non coinvolti.
- **Confidentiality**. Si riferisce alla capacità di nascondere il contenuto dei dati o di controllare la divulgazione degli stessi (ad esempio, il trasferimento di e-mail crittografate, l'applicazione del controllo di accesso a un documento classificato o a un database contenente informazioni sensibili). NIST descrive la riservatezza come la capacità di mantenere le restrizioni autorizzative all'accesso e alla divulgazione delle informazioni, compresi i mezzi per proteggere la privacy e le informazioni proprietarie. Sebbene la riservatezza sia una proprietà di sicurezza, come si evince dalla definizione, essa è importante anche per preservare le proprietà dell'anonimato e di inscindibilità.
- **Content awareness**. Si riferisce alla capacità di garantire che gli utenti abbiano la consapevolezza dei propri dati personali e di limitare l'uso delle informazioni necessarie per consentire l'esecuzione della funzione a cui si riferiscono. Quanto più sono elevate le informazioni personali identificabili divulgate dagli interessati, tanto maggiore è il rischio di violazione della privacy. L'utente deve essere consapevole delle conseguenze della condivisione delle proprie informazioni. Tali conseguenze possono riferirsi alla violazione della privacy così come a risultati indesiderati ottenuti fornendo informazioni incomplete o errate.
- **Policy and consent compliance**. Si riferisce alle politiche in atto e alle caratteristiche di conformità sul consenso in merito al trattamento dei dati personali per informare l'interessato sulla politica di privacy del sistema, o consentire allo stesso di specificare i consensi in conformità con la legislazione, prima che gli utenti stessi accedono al sistema.

Le proprietà sopra descritte possono essere considerate tutte proprietà tipiche di sicurezza.
Relativamente ai modelli di hard/soft privacy possono essere inoltre così suddivise:

- unlinkability, anonimity, pseudonymity, plausible deniability, undetectability and unobservability e confidentiality possono essere considerate come proprietà di hard privacy;
- content awareness, policy and consent compliance, possono essere considerate come proprietà di soft privacy.

5.8.1.2 Principi

La **Privacy by Design** è un concetto sviluppato alla fine degli anni 90 da Ann Cavoukian [3], commissario per l'informazione e la privacy dell'Ontario. Si tratta di un approccio ingegneristico che si concentra sull'intero processo a partire dai principi di privacy e protezione dei dati.
La tutela della privacy non dovrebbe essere garantita solo dal rispetto delle norme e dai quadri normativi, in quanto non vi è alcuna utilità nelle norme giuridiche riguardo una codifica rigorosa se il sistema stesso non ha una solida base per la sicurezza e la tutela della privacy.