cookie, ed è quindi spesso indicata come la "direttiva sui cookie". Inoltre, la direttiva disciplina lo spam online imponendo un regime di “opt-in”, in base al quale le e-mail indesiderate possono essere inviate solo previo accordo del destinatario. La direttiva comprende anche la conservazione e il trattamento dei dati relativi al traffico e dei dati relativi all'ubicazione. I dati relativi al traffico dovrebbero essere cancellati o resi anonimi non appena questi non sono più necessari ai fini della trasmissione. Il trattamento di tali dati può avvenire solo quando questi vengono resi anonimi o quando l'interessato ha fornito il proprio consenso.
Sebbene la legislazione sulla protezione dei dati sia complessa e spesso ambigua, alcune norme possono essere automatizzate nei sistemi software. Negli ultimi anni è emersa una ricerca che si propone di estrarre diritti e obblighi dai documenti legali e che fornisce la tracciabilità tra le politiche sulla privacy (scritte) e le loro controparti implementate nel software.

5.8.1.1 Proprietà

In quanto concetto astratto e soggettivo, la declinazione della privacy varia a seconda delle problematiche sociali e culturali, delle discipline di studio, degli interessi degli stakeholder e del contesto applicativo. Le norme di privacy più comuni sono volte a consentire agli individui di controllare, modificare, gestire e cancellare informazioni su se stessi e decidere quando, come e in quale misura tali informazioni possono essere comunicate agli altri.
La privacy si basa prevalentemente su due modelli di tutela:

- *hard privacy* (la privacy quale libertà negativa). Si basa sul concetto di libertà (e del relativo diritto) definendo un perimetro entro cui l’individuo può agire al riparo da invasioni esterne. Questa libertà dal controllo si esprime in una sfera di libertà di scelte e di comportamenti. Nella modellazione delle minacce è necessario tener conto delle seguenti entità: il fornitore di servizi, il titolare dei dati e l'ambiente con cui interagisce.
- *soft privacy* (privacy quale libertà positiva). Contrariamente al primo, si basa sul presupposto che l'interessato abbia concesso il controllo dei propri dati personali a terzi, e debba fidarsi dell'onestà e della competenza dei responsabili del trattamento. L'obiettivo di tale modello è quindi, di fornire la sicurezza dei dati ed elaborare questi con finalità e consenso specifici, tramite politiche, controllo degli accessi e audit. Il modello prevede che l'interessato fornisca i suoi dati personali e il responsabile del trattamento di tali dati è anche responsabile della loro protezione. Di conseguenza, si applica un modello di minaccia più debole, che include diverse parti con diversi poteri.

Alla base del modello di privacy, sono presenti alcune delle classiche proprietà di sicurezza quali:

- **confidenzialità,** garantisce che le informazioni siano accessibili solo da parte di persone autorizzate;
- **integrità,** garantisce la legittimità, l'accuratezza e la completezza delle informazioni e dei metodi di elaborazione;
- **disponibilità** (o resistenza alla censura), garantisce che le informazioni siano accessibili agli utenti autorizzati;
- **non ripudio,** garantisce che non si possa negare ciò che si è fatto.

Le caratteristiche di queste proprietà si trovano nella norma ISO 17799[37]. A queste si aggiungono ulteriori proprietà quali:

- **Unlinkability**. Si riferisce alla capacità di nasconde il legame tra due o più azioni (ad esempio, nascondere i link tra due messaggi anonimi inviati dalla stessa persona), identità (ad esempio, due pagine web visitate da parte dello stesso utente o due persone collegate da una relazione di amicizia in un social network) o informazioni (ad esempio, voci presenti in due distinti database relativi alla stessa persona). La unlinkability consiste nel separare due o più elementi di interesse, detti IOI, (quali ad esempio, soggetti, messaggi, azioni, etc). Questa separazione garantisce che all'interno del

[37] https://www.iso.org/standard/39612.html