potrebbe essere: "I membri del settore di ricerca e sviluppo possono consultare le informazioni riguardanti le abitudini di utilizzo di un prodotto di un singolo individuo per lo sviluppo di un nuovo prodotto se il soggetto in questione ha espresso esplicitamente il proprio consenso a rilasciare i propri dati in tal senso". Da notare che questa istruzione comprende la scelta da parte del proprietario delle informazioni di stabilire come utilizzare le proprie informazioni. È possibile, inoltre, applicare anche altre dipendenze per l'accesso alle informazioni personali. Ad esempio, una norma può imporre alcune restrizioni sull'utilizzo dei dati raccolti.
La privacy by Design è emersa come un approccio proattivo, integrativo e creativo per rafforzare i requisiti di privacy sin dalle prime fasi della progettazione applicativa. Tra le sfide legate all'ingegneria della privacy by design vi è la mancanza di metodologie olistiche, sistematiche e integrative che affrontino la complessità e la variabilità della privacy e sostengano la traduzione dei suoi principi fondamentali nelle attività di ingegneria. Per certi versi questo è comprensibile poiché l'approccio è stato sviluppato per tener conto di una serie di fonti normative e standard. Tuttavia, ne consegue che i suoi principi fondanti sono dati ad un alto livello di astrazione senza fornire a corredo metodologie e linee guida per ottenere requisiti concreti in materia di privacy. I principi fondamentali della Privacy by Design si basano sui Fair Information Practice Principles (FIPP) e fungono da framework universale per l'integrazione della privacy in tre principali aree di applicazione: tecnologie dell'informazione e della comunicazione, aree di business, progetti fisici e infrastrutturali.
La Privacy Engineering si è affermata come una nuova disciplina che mira ad applicare principi e processi di ingegneria nello sviluppo, nell'implementazione e manutenzione dei sistemi, in modo sistematico e ripetibile, per raggiungere un livello accettabile di protezione della privacy. Per distinguere tali concetti; la Privacy by Design (PbD) intende spiegare "Cosa fare" per raggiungere un livello adeguato di protezione della privacy, mentre la Privacy Engineering (PE) intende spiegare "Come farlo" definendo la privacy come un attributo di qualità nell'ingegneria dei sistemi. In altre parole, la PE si concentra sullo sviluppo e la valutazione di metodi, tecniche e strumenti che identificano e affrontano in modo sistematico le problematiche legate alla privacy durante il processo di sviluppo dei sistemi.
La tabella che segue, sintetizza i 'concetti' alla base della Privacy:

Concetto di Privacy	Descrizione
Personal Data	Informazioni che possono essere ricondotte ad un individuo.
Identifiable Natural Person	Individuo collegato al "Personal Data".
Item of Interest (IOI)	Informazioni relative ad un individuo (ad esempio soggetti, messaggi, azioni, ecc.).
Unlinkability	Impossibilità di distinguere se due IOI sono correlati.
Anonymity	Impossibilità di identificare il soggetto all'interno di un gruppo di soggetti.
Plausible deniability	Possibilità di negare di aver eseguito un'azione.
Undetectability	Impossibilità di distinguere se esiste un IOI.
Unobservability	Impossibilità nell'essere rintracciabili da tutti i soggetti coinvolti.
Confidentiality	Restrizioni autorizzative all'accesso e alla divulgazione delle informazioni.
Awareness	Essere consapevoli delle conseguenze della condivisione delle informazioni personali (vedi sopra, Personal Data).
Compliance	Aderenza alle normative e alle politiche interne di una organizzazione.

Tabella 23 - Concetti alla base della Privacy

Similmente alla miriade di normative sulla privacy disponibili, ci sono stati diversi tentativi di strutturare e classificare i concetti di privacy. Di seguito si riportano alcuni esempi di tassonomie basate su due approcci distinti:

- Classificazione dei concetti di privacy da un punto di vista giuridico;
- Classificazione dei concetti di privacy da un punto di vista di ingegneria del software.

Tassonomia di Solove. Presenta una tassonomia delle violazioni della privacy da un punto di vista legale. Anche se questa non tratta la privacy digitale, ma descrive la privacy in generale, fornisce comunque alcune informazioni utili in materia. Solove[36] opera una distinzione tra quattro gruppi di attività di base dannose:

- Raccolta dei dati. Include due tipi di violazioni della privacy: il controllo inteso come "osservazione, ascolto o registrazione delle attività di un individuo", e, l'investigazione che consiste in varie forme di sondaggio per ottenere informazioni.
- Trattamento dei dati. Include cinque tipi di violazioni dei dati raccolti al punto precedente: aggregazione (ovvero combinazione di dati relativi a un individuo), identificazione (ovvero collegamento dei dati per identificare un individuo), negligenza (poca attenzione nella protezione dei dati memorizzati), uso secondario (ovvero utilizzo dei dati per scopi diversi da quelli per i quali sono stati raccolti) ed esclusione (ovvero quando l'interessato non è a conoscenza di dati che lo riguardano che gli altri posseggono).
- Diffusione dei dati. Include sette categorie di violazioni: violazione della riservatezza (ovvero non mantenere riservate le informazioni di una persona), divulgazione (cioè rivelare informazioni "sensibili" veritiere su una persona), esposizione (cioè rivelare le nudità, il dolore o le caratteristiche fisiche di una persona), maggiore accessibilità (cioè amplificare l'accessibilità dei dati), appropriazione (cioè l'uso della propria identità per perseguire un'altra finalità).
- Invasione. A differenza dei gruppi precedenti, non riguarda necessariamente le informazioni personali, ma degli elementi che limitano la sfera personale e decisionale (ad esempio atti invasivi che violano la tranquillità di una persona e che impattano sulle decisioni private di una persona).

Linee guida FIPPs (Fair Information Practice Principles). La Privacy and Personal Information Protection raccoglie un insieme di indicazioni proposte dalla Federal Trade Commission degli Stati Uniti. Queste possono essere considerate come il fondamento di tutta la legislazione vigente negli Stati Uniti, in materia di protezione dei dati. Sono state utilizzate per la definizione delle linee guida dell'OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) e per la direttiva europea sulla protezione dei dati. I principi si basano su cinque distinte categorie:

- Avviso/Consapevolezza. I soggetti interessati dovrebbero essere adeguatamente informati prima di procedere nella raccolta delle informazioni personali che li riguardano.
- Scelta/Consenso. I soggetti interessati devono essere in grado di scegliere come devono essere utilizzati i propri dati personali. In particolare laddove si fa un uso secondario dei dati (ad esempio, registrazione ad una mailing list o trasferimento di informazioni a terzi).
- Accesso/Partecipazione. Una persona dovrebbe essere in grado di accedere ai dati che la riguardano e di contestarne l'accuratezza e la completezza.
- Integrità/Sicurezza. I dati devono essere accurati e protetti.
- Enforcement/Redress. Dovrebbero essere messe in atto misure di enforcement per garantire il rispetto dei FIPP.

Le FIPP sono utilizzate anche per definire altre tassonomie di privacy. Se ne cita qualcuna a titolo di esempio:

[36] https://en.wikipedia.org/wiki/Daniel_J._Solove

- linee guida Microsoft per la privacy;
- tassonomia definita da Anton et al.[13]. Questa tassonomia però, non contiene solo i cinque FIPP come obiettivi di protezione della privacy, ma include anche una serie di obiettivi di vulnerabilità di privacy che sono correlati alle minacce esistenti. Questi obiettivi di vulnerabilità includono il monitoraggio delle informazioni, l'aggregazione, la memorizzazione, il trasferimento di informazioni, la raccolta e la personalizzazione.

European Data Protection Legislation. La legislazione è una questione complessa, spesso vaga e formulata in modo ambiguo; il che la rende molto difficile da attuare. La privacy non richiede solo misure tecnologiche, ma anche misure organizzative. Inoltre, è difficile prevedere tutti i potenziali domini e contesti (e le relative normative) in cui un prodotto software verrà poi utilizzato. Tuttavia, alcune disposizioni legislative in materia di protezione dei dati possono, con un minimo sforzo, essere integrate nella progettazione del sistema.
Guarda e Zannone [2] riassumono la Direttiva Europea sulla Protezione dei Dati nei seguenti nove principi:

- Elaborazione corretta e lecita. La raccolta e il trattamento dei dati personali non devono interferire in modo irragionevole con la privacy delle persone interessate né interferire in modo irragionevole con la loro autonomia e integrità e devono essere conformi al quadro giuridico generale.
- Consenso. I dati personali devono essere raccolti e trattati solo previo esplicito consenso al loro trattamento da parte degli interessati.
- Finalità. I dati personali devono essere raccolti per finalità specifiche, lecite e legittime e non devono essere trattati per finalità non compatibili con quelle per cui sono stati raccolti.
- Minimalità. La raccolta e il trattamento dei dati personali sono limitati al minimo necessario per il raggiungimento delle finalità specifiche. Ciò include che i dati personali vengono conservati solo per il tempo necessario a raggiungere lo scopo specifico.
- Informazione minima. La divulgazione di dati personali a terzi deve essere limitata e deve avvenire solo a determinate condizioni.
- Qualità dell'informazione. I dati personali devono essere accurati, pertinenti e completi rispetto alle finalità per le quali sono raccolti e trattati.
- Controllo dell'interessato. L'interessato deve essere in grado di controllare e condizionare il trattamento dei suoi dati personali.
- Sensibilità. Nel trattamento dei dati personali è necessario applicare misure di protezione maggiormente rigorose su quei dati ritenuti particolarmente sensibili per il soggetto interessato.
- Sicurezza delle informazioni. I dati personali devono essere trattati in modo da garantire un livello di sicurezza adeguato ai rischi connessi al trattamento e alla natura dei dati stessi.

Poiché il DPD è stato creato in un momento in cui Internet era ancora agli inizi, nel 2012 è stata elaborata una proposta di riforma della legislazione attuale per rafforzare i diritti della privacy online. Questa riforma indirizza:

- il "diritto all'oblio" ovvero, l'obbligo di fornire esplicitamente il consenso necessario al trattamento dei dati;
- il "diritto di portabilità dei dati" che consente un accesso più facile ai propri dati e una maggiore trasparenza sul modo in cui questi vengono gestiti.

Anche la responsabilità di coloro che trattano i dati personali è accresciuta dall'attuazione di principi quali "Privacy by Design".
La direttiva relativa alla privacy e alle comunicazioni elettroniche è stata promulgata nel 2002 e completa la direttiva DPD in quanto si concentra sulla protezione dei dati nell'era digitale. Essa disciplina il settore delle comunicazioni elettroniche ed è stata modificata nel 2009. È principalmente nota per la richiesta di consenso da parte dell'utente nella memorizzazione dei