ANNO ACCADEMICO 2024/2025

Etica, Società e Privacy

Privacy

Altair's Notes

UNIVERSITÀ DI TORINO

DIPARTIMENTO DI INFORMATICA

Premessa

Licenza

Formato utilizzato

Box di "Concetto sbagliato":

Concetto sbagliato 0.1: Testo del concetto sbagliato

Testo contente il concetto giusto.

Box di "Corollario":

Corollario 0.0.1 Nome del corollario

Testo del corollario. Per corollario si intende una definizione minore, legata a un'altra definizione.

Box di "Definizione":

Definizione 0.0.1: Nome delle definizione

Testo della definizione.

Box di "Domanda":

Domanda 0.1

Testo della domanda. Le domande sono spesso utilizzate per far riflettere sulle definizioni o sui concetti.

Box di "Esempio":

Esempio 0.0.1 (Nome dell'esempio)

Testo dell'esempio. Gli esempi sono tratti dalle slides del corso.

Box di "Note":

Note:-

Testo della nota. Le note sono spesso utilizzate per chiarire concetti o per dare informazioni aggiuntive.

Box di "Osservazioni":

Osservazioni 0.0.1

Testo delle osservazioni. Le osservazioni sono spesso utilizzate per chiarire concetti o per dare informazioni aggiuntive. A differenza delle note le osservazioni sono più specifiche.

1 Privacy - Introduzione

1.1 Il Corso in Breve...

Obiettivi:

- Riconoscere problemi di privacy nella modellazione e nell'analisi dei dati.
- Conoscenza di base su metodi per preservare la privacy.

Syllabus:

1. Il concetto di privacy e le leggi sulla privacy in differenti paesi.
2. Le sfide della privacy nell'era dei Big Data.
3. Sistemi di informazione.
4. Modelli statistici.
5. Attacchi alla privacy e modelli di anonimizzazione in database statistici.
6. Privacy differenziale.
7. Separazione dei dati.

1.2 Privacy e Leggi sulla Privacy

1.2.1 Che Cos'è la Privacy?

Domanda 1.1

Che cos'è la privacy?

Definizione 1.2.1: Privacy 1

La *privacy* può essere definita come il diritto a stare da soli.

Warren and Brandeis (1890), *The Right to Privacy*:

- Una delle tesi più influenti nella storia americana.
- GLi autori tentarono di trovare un modo di descrivere legalmente la privacy.

Note:-

Esempio: il diritto di una persona a scegliere la seclusione dalle attenzioni altrui, il diritto di non essere osservati nella sfera privata.

Definizione 1.2.2: Privacy 2

La *privacy* può essere definita come accesso limitato alle informazioni.

- Una persona deve essere libera di scegliere in che misura partecipare alla società senza che gli altri debbano sapere.
- Godkin (1880): “nothing is better worthy of legal protection than private life, or, in other words, the right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion.”.
- Bok (1989): la privacy è "the condition of being protected from unwanted access by others—either physical access, personal information, or attention.".

Definizione 1.2.3: Privacy 3

La *privacy* può essere vista come controllo sull’informazione.

- Westin and Blom-Cooper (1970): "privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.“.
- Fried (1968): "Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.”.

Definizione 1.2.4: Privacy FIPS PUB 41

Il diritto di un’entità ... a determinare il grado con il quale interagire con il proprio ambiente, compreso il grado con cui un’entità voglia condividere informazioni personali con gli altri.

Definizione 1.2.5: Privacy ISO

Il diritto di un individuo a controllare o influenzare quali informazioni collegate a loro possono essere collezionate e salvate e da chi e a chi queste informazioni possono essere accedute.

Osservazioni 1.2.1

Definizioni derivabili:

- La privacy è l’abilità di una persona di controllare la disponibilità di *informaziioni* e la sua *esposizione*.
- È collegata a essere abili a funzionare in una società *anonimamente*.

Edward Snowden files: viene pubblicato il file contente le informazioni riguardo i dati raccolti dal NSA riguardo le chiamate di milioni di privati cittadini.

1.2.2 Perché la Privacy è Così Importante?

Domanda 1.2

Perché la privacy è così importante?

La privacy è importante perché:

- *Sentimenti individuali:*
  - Non confortabile: possesso dell'informazione.
  - Non sicuro: l'informazione può essere usata in modo improprio (furto d'identità).
- *Le aziende hanno bisogno di:*
  - Far si che i loro clienti si sentano al sicuro.
  - Mantenere una buona reputazione[1].
  - Proteggere sé stesse da ogni disputa legale.
  - Obbedire alle leggi.

Tipi di privacy:

- Political privacy.
- Consumer Privacy.
- Medical privacy.
- Private property.
- Information/Data privacy.

Definizione 1.2.6: Data Privacy

Il problema della *data privacy* emerge quando dei dati unicamente associabili a un individuo sono collezionati e salvati.

Le fonti più comuni di dati affetti da data privacy:

- Record sanitari.
- Investigazioni e processi criminali.
- Transazioni finanziarie.
- Tratti biologici (e. g. materiale genetico).
- Residenza e posizione geografica.
- Geolocalizzazione.
- Utilizzo del web.

Osservazioni 1.2.2

- La sfida della data privacy è trovare un modo per *condividere dati* proteggendo le informazioni che permettono di identificare una determinata persona.
  - Per esempio negli ospedali i dati vengono trasferiti in maniera aggregata.
  - L'idea di condividere i dati in forma aggregata garantisce che solo dati non identificabili sono condivisi.
- La protezione legale deò diritto alla privacy *cambia drasticamente a seconda della nazione*.

[1] Beh, visto che merda sono Twitter e META non credo gliene freghi qualcosa.

1.2.3 Privacy negli Stati Uniti

La data privacy *non è molto regolata* negli USA:

- Non c'è una legge che controlli tutti gli aspetti dei dati (acquisizione, collezione, trattamento e uso).
- Se un'azienda colleziona dei dati (anche senza permesso) ha il diritto di utilizzarli.
- Gli istituti possono informarsi sulle condizioni finanziarie di una persona (banche, assicurazioni, etc.) chiedendo report a terze parti.
- Ci sono alcune eccezioni:
  - Dati sanitari (HIPAA).
  - Dati dei bambini sotto i 13 anni online (COPPA).
  - Richieste di prestito (FCRA).
  - Sicurezza informatica (ECPA, PATRIOT[2], etc.).

1.2.4 Privacy nell'Unione Europea

La data privacy nell'UE *è pesantemente regolata*:

- l'articolo 8 della convenzione europea sui diritti umani (ECHR) prevede il diritto al rispetto della privacy di una persona (poter disporre di una sfera privata, una vita familiare, un domicilio e della propria corrispondenza).
- La corte dei diritti umani ha dato a quest'articolo varie interpretazioni, con le seguenti eccezioni:
  - Ottenere informazioni per censimenti ufficiali.
  - Raccogliere impronte digitali e fotografie per attività di polizia.
  - Collezionare dati medici e spese personali.
  - Implementare sistemi di identificazione personale (un documento di identificazione).

Note:-

Spesso questa maggiore tutela della privacy viene criticata dalle aziende che la vedono come un freno al progresso.

Ci sono state due ere della privacy:

- 1995-2018: Data Protection Directive (DPD).
- 2018-presente: General Data Protection Regulation (GDPR[3]).

Definizione 1.2.7: Data Protection Directive

La Data Protection Directive (DPD) fu adottata nel 1995 dal parlamento europeo:

- Come tentativo di armonizzare la protezione dei dati nell'unione europea.
- Doveva essere regolamentata da leggi nazionali nel 1998.

[2] Nel 2001, in seguito a un certo evento terroristico.
[3] Promulgato nel 2016, ma diventato effettivo dal maggio del 2018

Gli 8 princìpi di base del DPD:

1. I dati personali devono essere processati a norma di legge e in maniera corretta.
2. I dati personali devono essere processati solo per certi scopi limitati.
3. I dati personali devono essere processati in modo adeguato, rilevante e non eccessivo.
4. I dati personali devono essere processati accuratamente.
5. I dati personali devono essere trattenuti solo per il tempo strettamente necessario.
6. I dati personali devono essere processati in accordo con i diritti del soggetto interessato.
7. I dati personali devono essere processati in modo sicuro.
8. I dati personali devono essere trasferiti solo a nazioni con una protezione adeguata.

Definizione 1.2.8: Personal Data - DPD

Ogni informazione relativa a una persona identificata i identificabile. Una persona identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare identificando un particolare numero di identificazione o uno o più fattori fisici, psicologici, mentali, economici, culturali o sociali.

Note:-

Questa definizione viene rafforzata nel GDPR.

Definizione 1.2.9: Data Processing - DPD

Ogni operazione o insieme di operazioni che viene effettuata su dati personali, tramite un mezzo automatizzato o meno, come la collezione, registrazione, organizzazione, immagazzinamento, adattamento o alterazione, recupero, consultazione, uso, trasmissione, disseminazione o altra distribuzione, allineamento o combinazione, blocco, cancellazione o distruzione.

Note:-

Vengono effettuati cambiamenti minori nel GDPR.

Definizione 1.2.10: Responsabile - DPD

Il responsabile può essere una persona fisica o giuridica, un autorità pubblica o un ente che deve garantire l'integrità dei dati trattati.

Corollario 1.2.1 Processore

Il processore dei dati è una persona fisica o giuridica, un'autorità pubblica, un'agenzia o qualunque altro ente che processa i dati personali per conto del responsabile.

Note:-

Non ci sono cambiamenti nel GDPR.

Princìpi della gestione dei dati. I dati personali non dovrebbero essere processati a meno che non riguardino queste categorie:

- *Trasparenza*: il soggetto dei dati ha il diritto di essere informato da un'azienda che sta elaborando i suoi dati personali.
- *Scopo legittimo*: i dati personali possono essere processati solo per scopi legittimi e non usati per altri scopi non pertinenti.
- *Proporzionalità*: i dati personali processati devono essere adeguati, rilevanti e non eccessivi in relazione allo scopo per quale i dati vengono collezionati e ulteriolmente processati.

Trasparenza:

- Il soggetto dei dati deve dare il *consenso*.
- Il processamento era necessario per l'*esecuzione di un contratto*.
- Il processamento era necessario per *assolvere un obbligo legale*.
- Il processamento era necessario per *proteggere gli interessi vitali* del soggetto dei dati.
- Il processamento era necessario per un'operazione di *interesse pubblico*.
- Il processamento era necessario per *scopi di interesse legittimato dal controllore, eccetto quando quegli interessi sono sovrascritti dagli interessi dei diritti fondamentali e della libertà del soggetto*.

Osservazioni 1.2.3

Il soggetto ha il diritto a:

- Accedere a tutti i dati su di lui/lei/loro.
- Domandare la rettifica, cancellazione o blocco dei dati se sono incompleti, inaccurati o non sono processati come previsto dalle regole sulla protezione dei dati.

Proporzionalità:

- I dati devono essere accurati e, quando necessario, aggiornati.
- I dati non devono essere mantenuti in una forma che permette l'identificazione del soggetto per più tempo del necessario.
- Gli stati membri hanno la possibilità di memorizzare i dati personali per fini statistici o scientifici.
- Vengono applicate tutele aggiuntive per la gestione dei *dati sensibili* (credenze religiose, opinioni politiche, salute, orientamento sessuale, gruppo etico, appartenenza a organizzazioni).
- Il soggetto può sempre chiedere la cancellazione dei suoi dati usati per fini pubblicitari[4].
- Qualunque decisione automatizzata sulla persona non deve essere fatta in maniera completamente automatica.
- L'individuo può *fare ricorso* su qualsiasi decisione automatica in cui vengono processati i propri dati.

Autorità della privacy:

- Ogni stato membro deve eleggere un'*autorità di supervisione* che:
  - Deve *monitorare la protezione dei dati* in quello stato membro.
  - Dare *avvisi al governo riguardo le misure amministrative e i regolamenti*.
  - *Iniziare procedure legali* quando il regolamento sulla protezione dei dati viene violatao.
- Il *controllore* deve notificare all'autorità di supervisione le seguenti informazioni:
  - Il nome e l'indirizzo del controllore.
  - Lo scopo del processamento.
  - Una descrizione delle categorie dei dati del soggetto.
  - Il recipiente a cui i dati possono essere inotrati.
  - Proposte di trasferimento dei dati a stati terzi.
  - Una descrizione generale delle misure prese per garantire la sicurezza dei dati processati.
- Le informazioni sono tenute in un *registro pubblico*.

[4] Contrariamente agli stati uniti.

Leggi della privacy in Italia:

- Il DPD è stato implementato con il decreto legislativo 196/2003 (Codice in materia di protezione dei dati personali).
- Inoltre il Garante per la protezione dei dati limitati doveva applicare misure appropriate in determinati campi (video sorveglianza, dati biometrici, dati sanitari, notifiche di data breach, informazioni bancarie, profili online, processamenti fatti da amministratori di sistema, processamenti a fini di marketing e profiling, pagamenti elettronici, cookies).

Definizione 1.2.11: General Data Protection Regulation

La General Data Protection Regulation (GDPR) è un regolamento attraverso il quale l'unione europea intende aumentare la forza e unificare la protezione dei dati per tutti gli individui all'interno dell'unione europea.

Note:-

L'obiettivo principale del GDPR è quello di offrire un controllo semplificato agli appartenenti ai paesi membri dell'unione europea.

Definizione 1.2.12: Personal Data - GDPR

Uguale al DPD, ma aggiunge come caratteristiche di identificazione i dati di locazion, gli identificatori online, lo stato genetico, economico e culturale.

Definizione 1.2.13: Data Processing - GDPR

Uguale al DPD, ma viene inclusa la "strutturazione" dei dati processati.

Note:-

Inoltre il GDPR include altre definizioni.

Definizione 1.2.14: Pseudoanimizzazione

La pseudoanimizzazione è il processamento in cui i dati personali non possono più essere attribuiti univocamente a un soggetto senza informazioni aggiuntive. Le informazioni aggiuntive sono tenute separate e soggette a misure tecniche e organizzative per assicurare che i dati siano anonimi.

La pseudoanimizzazione:

- Se viene effettuata con politiche adeguate non è soggetto a controlli e penalità.
- La regolamentazione non coinvolge dati usati per statistiche o ricerche.
- Le politiche e le misure che raggiungono la privacy by Design e la privacy by Default sono adeguati.

Definizione 1.2.15: Personal Data Breach

Un leak accidentale nella sicurezza per cui il dato personale viene distrutto, perso, alterato, rubato o acceduto.

Diritti del soggetto:

- L'individuo deve dare un *consenso chiaro* per il trattamento dei propri dati.
- Il soggetto ha un *facile accesso* ai propri dati.
- Viene evidenziato il diritto alla rettifica, alla cancellazione e all'oblio[5].

[5] Cosa non facile, soprattutto con i social.

- Il diritto di obiezione, incluso l'utilizzo dei propri dati per "profiling".
- Il diritto alla portabilità dei dati da un servizio a un altro.

Privacy *by Design* e *by Default*:

- Viene richiesto che la protezione dati sia presente fin dall'inizio nel sistema informativo.
- Le impostazioni della privacy devono essere di alto livello.
- La privacy deve essere presente per tutto il ciclo di vita del processamento dei dati.
- Come già detto i dati personali devono essere processati solo quando è necessario per ogni specifico scopo.

Definizione 1.2.16: Privacy by Design - Ann Cavoukian

Un approccio all'ingegneria dei sistemi che tiene in considerazione la privacy durante tutto il ciclo di vita. Si basa su 7 princìpi fondamentali:

1. Proattività, non reattività (prevenzione, non rimedio).
2. Privacy come impostazione di Default.
3. Privacy integrata nel Design.
4. Completamente funzionale.
5. End-to-end security.
6. Visibilità e trasparenza.
7. Rispetto per la privacy degli utenti.

Responsabilità:

- Il titolare del trattamento del dato deve dimostrare che tutte le operazioni messe in atto per garantire la sicurezza del dato siano aderenti alla legge.
- È responsabilità del controllore dei dati di implementare misure effettive e di dimostrare la *compliance* alle attività di processamento.
- L'utente deve essere chiaramente informato riguardo le finalità del trattamento, alla legge usata come base, all'intervallo temporale del trattamento, se i dati vengono trasferiti a terze parti e se avvengono delle decisioni automatizzate.
- Viene introdotto il *Data Protection Officer*, un esperto tecnico del dato e legale del GDPR.
- Se avvengono eventi di rischio bisogna fare un *Data Protection Impact Assessments* (DPIA) per valutarne l'estensione.
- La valutazione e la mitigazione del rischio sono necessarie e approvazione delle autorità nazionali di protezione dei dati (DPA) è necessario per rischi elevati.
- I records delle attività di trattamento devono essere conservate in modo includere le finalità del trattamento, le categorie coinvolte e Termini previsti.
- I records devono essere disponibili all'autorità di supervisione, su richiesta.

Definizione 1.2.17: Data Protection Officer

Il GDPR stabilisce la figura del Data Protection Officer (DPO), una persona con conoscenze specialistiche in materia di protezione dei dati e pratiche che dovrebbero aiutare il titolare del trattamento o l'incaricato del trattamento a monitorare conformità interna al presente regolamento. The DPO are also expected to be proficient at managing IT processes, data security (including dealing with cyber-attacks) and other critical business continuity issues around the holding and processing of personal and sensitive data.

Note:-

Autorità pubbliche e imprese le cui attività principali sono trattamento regolare o sistematico dei dati personali, sono necessario per assumere un DPO.

Definizione 1.2.18: Data Breach

Il controllore dei dati ha l'obbligo legale di notificare l'autorità di supervisione senza ritardi non necessari, a meno che sia improbabile che il data breach causi rischi alla libertà e ai diritti dell'individuo. C'è un massimo di 72 ore dopo aver scoperto il data breach per notificare.

Le seguenti sanzioni possono essere imposte:

- Nel primo e non intenzionale caso di noncompliance viene emesso un avviso.
- Una multa fino a 10 milioni di euro o fino al 2% dell'annualità mondiale fatturato dell'esercizio finanziario precedente nel caso di un'impresa, se vi è stata una violazione di alcuni obblighi.
- Una multa fino a 20 milioni di euro o fino al 4% dell'annuo in tutto il mondo fatturato dell'esercizio finanziario precedente nel caso di un'impresa, se vi sono state gravi violazioni dei princìpi.

1.2.5 Regolamenti Transazionali

- Safer Harbor privacy principles (fino al 2015).
- EU-US Privacy Shield (2016-2020[6]).
- EU-US Data Privacy Framework (2023-presente).

Definizione 1.2.19: Safe Harbor

Sviluppato tra il 1998 e il 2000 al fine di impedire alle organizzazioni private di l'UE o gli Stati Uniti dalla divulgazione accidentale o dalla perdita di informazioni personali.

Le compagnie USA che tengono dati devono aderirea questi 7 princìpi:

1. *Notifica*: gli individui devono essere informati che i loro dati stanno venendo collezionati e come verranno usati.
2. *Scelta*: gli individui possono scegliere di rimuovere i propri dati rinunciando ai servizi[7].
3. *Trasferimento*: la trasmissione dei dati a terzi può avvenire solo ad altri organizzazioni che seguono principi di protezione dei dati adeguati.
4. *Sicurezza*: bisogna evitare la perdità di informazioni collezionate.
5. *Data Integrity*: i dati devono essere rilevanti e affidabili per lo scopo per cui sono raccolti.
6. *Accesso*: gli individui devono essere in grado di accedere, correggere e cancellare i propri dati.
7. *Applicazione*: devono esistere mezzi efficaci per far rispettare queste norme.

[6] Caduto a causa del primo governo Trump.
[7] Google merda.

Breve storia di Safe Harbor:

- Nel 2000 la Commissione europea ha deciso che il principi degli Stati Uniti erano conformi alla direttiva dell'UE (la cosiddetta "Decisione Safe Harbor").
- Dopo che un cliente si è lamentato del fatto che i suoi dati di Facebook non erano sufficientemente protetti la corte di giustizia della commissione europea, nel 2015, dichiara la decisione di Safe Harbor invalida.
- La Commissione ha tenuto ulteriori colloqui con gli Stati Uniti autorità competenti verso "un quadro rinnovato e solido per flussi di dati transatlantici".
- La Commissione europea e gli Stati Uniti hanno convenuto di istituire un nuovo quadro per i flussi transatlantici di dati il 2 febbraio 2016, noto come "EU-US Privacy Shield".

Definizione 1.2.20: EU-US Privacy Shield

Lo scudo UE-USA per la privacy è un quadro per gli scambi transatlantici di dati per finalità commerciali tra l'Unione Europea e gli Stati Uniti. Uno dei suoi scopi è quello di consentire alle aziende statunitensi di ricevere più facilmente dati provenienti da entità dell'UE ai sensi delle leggi sulla privacy dell'UE volte a proteggere i cittadini dell'unione europea.

Osservazioni 1.2.4

- La Commissione europea ha adottato il quadro il 12 luglio 2016 ed è entrato in vigore lo stesso giorno.
- Il presidente degli Stati Uniti Donald Trump ha firmato un ordine esecutivo intitolato "Enhancing Public Safety", in cui si afferma che le protezioni della privacy degli Stati Uniti non saranno estese oltre i cittadini o residenti statunitensi.
- Nel luglio 2020 lo scudo UE-USA per la privacy è stato abrogato dalla Corte europea giustizia in quanto non forniva tutele adeguate ai cittadini dell'UE rispetto allo Snooping governativo americano[a].

[a] In poche parole gli americani si comportano da americani.

Definizione 1.2.21: AI Act

La legge sull'IA mira a garantire che i sistemi di IA utilizzati nell'UE siano sicuri, trasparenti e rispettosi diritti fondamentali.

L'AI Act classifica i sistemi di IA in base al livello di rischio che rappresentano:

- *Rischio inaccettabile*: i sistemi di IA che rappresentano una chiara minaccia per la sicurezza o i diritti fondamentali sono vietato. Ciò include i sistemi che implementano tecniche subliminali per manipolare il comportamento, sfruttare le vulnerabilità di gruppi specifici o abilitare il punteggio sociale da parte dei governi.
- *Alto rischio*: sistemi di intelligenza artificiale utilizzati in aree critiche come la sanità, l'istruzione, l'occupazione, il diritto l'applicazione delle norme e i servizi essenziali sono soggetti a obblighi rigorosi. Questi includono rigorosi valutazioni dei rischi, misure di governance dei dati, supervisione umana e monitoraggio continuo per garantire la conformità.
- *Rischio limitato*: i sistemi di intelligenza artificiale a rischio limitato, come i chatbot e i deepfake, sono soggetti a obblighi di trasparenza. I fornitori e i distributori devono informare gli utenti che stanno interagendo con un sistema di intelligenza artificiale.
- *Rischio minimo*: la maggior parte dei sistemi di intelligenza artificiale, come i videogiochi abilitati all'intelligenza artificiale o i filtri antispam, cadono rientrano in questa categoria e sono in gran parte non regolamentate, incoraggiando l'innovazione e lo sviluppo,