CBM | CATTANEO BIONDA MAZZUCCHELLI
STUDIO LEGALE E NOTARILE

«PROTEZIONE DELLA SFERA PRIVATA E DEI DATI IN RADIOLOGIA ALLA PROVA DELL'AI»

MANNO, 16 SETTEMBRE 2026

Avv. Gianni CATTANEO, LL.M.

www.cbm-lex.ch

gianni.cattaneo@cbm-lex.ch

© Gianni Cattaneo, 2026: tutti i diritti sono riservati. Sono vietati la riproduzione, la pubblicazione e la distribuzione non autorizzati.

AGENDA

1. Una premessa tecnica e una giuridica
2. La tutela della sfera privata
3. La protezione dei dati personali
4. Segreto professionale e segreto d'ufficio
5. Aspetti delicati e rischi; obblighi del titolare dell'elaborazione
6. Le decisioni individuali automatizzate
7. Bonus Track: Principali quesiti da porsi

AGENDA

1. Una premessa tecnica e una giuridica

- L' «AI» si declina in una miriade di tecnologie, ognuna con i propri rischi peculiari:
  - IA generativa **vs** IA agentica
  - Modello locale **vs** Piattaforma in Cloud (as a service) o API
  - Modello proprietario **vs** Modello «open-weights»
  - Integrata in dispositivi **vs** semplice App (software)
  - Generica **vs** specializzata (qualità dei dati di addestramento)
  - «Allucinazioni» / «black box»
  - «Incubo» per la sicurezza informatica
- Anche le finalità/modalità d'uso sono rilevanti:
  - Assistenza all'umano durante il processo decisionale
  - Verifica a posteriori della decisione umana
  - Sostituzione dell'umano: decisioni individuali automatizzate
  - Trattamento di informazioni confidenziali e/o dati personali

- Non tratterò temi di responsabilità e uso diligente, limitandomi a:
  - Rischi
  - Scelta
  - Organizzazione
  - Obblighi collegati

- Legge federale sulla protezione dei dati (LPD)

  Settore privato: relazione orizzontale clinica privata / medico – paziente

  OPDa: Standard minimi di sicurezza (implicazioni penali)

- Legge cantonale sulla protezione dei dati cantonali (LPDP) / Revisione totale LPDP: adottata il 15. 09. 2026!)

  Settore pubblico: relazione verticale ospedale pubblico – paziente

- Tutela della personalità e dei diritti fondamentali dei pazienti (Cst. / CEDU): **dignità** della persona, **centralità** dell'essere umano

- LPD/LPDP si applica all'implementazione dell'IA?

Traduci in inglese: Il mio cliente Riccardo Salvioni, uomo bianco (caucasico), in seguito all'operazione all'anca, ha deciso di votare per Trump.

> **Tragically, Hanff passed away in 2019 at the age of 48. Despite his untimely death, his legacy lives on through his work and the many individuals and organizations he inspired to take action on issues related to digital privacy and data protection.**

Pubblicato il 12 febbraio 2025

Regolamentazione dell'IA: il Consiglio federale intende ratificare la Convenzione del Consiglio d'Europa

Berna, 12.2.2025 - La Svizzera intende ratificare la Convenzione del Consiglio d'Europa sull'intelligenza artificiale (IA) e apportare le necessarie modifiche al diritto svizzero. Inoltre, occorre proseguire le attività di regolamentazione dell'IA in singoli settori, come nell'ambito sanitario e dei trasporti. Nella seduta del 12 febbraio 2025, il Consiglio federale si è espresso a favore di questo approccio.

Migliora il modello per tutti

Acconsenti all'uso dei tuoi contenuti per addestrare i nostri modelli, permettendo così a ChatGPT di essere più utile a te e a tutti i suoi utenti. Adottiamo le misure necessarie per tutelare la vostra privacy. Scopri di più

Do humans view my content?

A limited number of authorized OpenAI personnel, as well as trusted service providers that are subject to confidentiality and security obligations, may access user content only as needed for these reasons: (1) investigating abuse or a security incident; (2) to provide support to you if you reach out to us with questions about your account; (3) to handle legal matters; or (4) to improve model performance (unless you have opted out). Access to content is subject to technical access controls and limited only to authorized personnel on a need-to-know basis. Additionally, we monitor and log all access to user content and authorized personnel must undergo security and privacy training prior to accessing any user content.

Output from GPT-4:

exempted it from regulations, subsidized its operations and promoted its practices, records and interviews showed.
Their actions turned one of the best-known symbols of New York — its yellow cabs — into a financial trap for thousands of immigrant drivers. More than 950 have filed for bankruptcy, according to a Times analysis of court records, and many more struggle to stay afloat.
"Nobody wanted to upset the industry," said David Klahr, who from 2007 to 2016 held several management posts at the Taxi and Limousine Commission, the city agency that oversees medallions. "Nobody wanted to kill the golden goose."
New York City in particular failed the taxi industry, The Times found. Two former mayors, Rudolph W. Giuliani and Michael R. Bloomberg, placed political allies inside the Taxi and Limousine Commission and directed it to sell medallions to help them balance budgets and fund key initiatives.
During that period, much like in the mortgage lending crisis, a group of industry leaders enriched themselves by artificially inflating medallion prices. They encouraged medallion buyers to borrow as much as possible and ensnared them in interest-only loans and other one-sided deals that often required borrowers to pay hefty fees, forfeit their legal rights and give up most of their monthly incomes.
When the market collapsed, the government largely abandoned the drivers who bore the brunt of the crisis. Officials did not bail out borrowers or persuade banks to soften loan

Actual text from NYTimes:

exempted it from regulations, subsidized its operations and promoted its practices, records and interviews showed.
Their actions turned one of the best-known symbols of New York — its signature yellow cabs — into a financial trap for thousands of immigrant drivers. More than 950 have filed for bankruptcy, according to a Times analysis of court records, and many more struggle to stay afloat.
"Nobody wanted to upset the industry," said David Klahr, who from 2007 to 2016 held several management posts at the Taxi and Limousine Commission, the city agency that oversees cabs. "Nobody wanted to kill the golden goose."
New York City in particular failed the taxi industry, The Times found. Two former mayors, Rudolph W. Giuliani and Michael R. Bloomberg, placed political allies inside the Taxi and Limousine Commission and directed it to sell medallions to help them balance budgets and fund priorities. Mayor Bill de Blasio continued the policies.
Under Mr. Bloomberg and Mr. de Blasio, the city made more than $855 million by selling taxi medallions and collecting taxes on private sales, according to the city.
But during that period, much like in the mortgage lending crisis, a group of industry leaders enriched themselves by artificially inflating medallion prices. They encouraged medallion buyers to borrow as much as possible and ensnared them in interest-only loans and other one-sided deals that often required them to pay hefty fees, forfeit their legal rights and give up most of their monthly incomes.

IFPDT: i diritti fondamentali dei pazienti devono essere tutelati; nella scelta di sistemi, software e dispositivi basati su IA occorre valutare non solo la qualità del dispositivo (nel senso delle radiazioni emesse), bensì la conformità del dispositivo alle norme sulla protezione dei dati personali → «privacy by design»

AGENDA

2. La tutela della sfera privata

- La protezione della personalità contro lesioni illecite (art. 28 CC)
- *Chi è illecitamente leso nella sua personalità può, a sua tutela, chiedere l'intervento del giudice contro* ***chiunque partecipi all'offesa.***
- Nozione di «personalità»: «*Tutto ciò che serve ad individualizzare una persona e che è degno di protezione considerati i bisogni di relazione tra individui secondo i costumi*»
- Diritto morale e **assoluto**
- Teoria delle tre sfere (DTF 97 II 97):
  - **sfera segreta o intima**: «i fatti e le vicende della vita che devono essere sottratti alla conoscenza delle altre persone, ad eccezione di coloro cui tali fatti sono stati specialmente confidati, quali i conflitti famigliari, le attitudini sessuali e lo **stato di salute**»
  - **sfera privata**: «l'ambito generale della vita privata»

AGENDA

3. La protezione dei dati personali

- La protezione legale si applica a

  qualsiasi operazione relativa a dati personali, indipendentemente dai mezzi e dalle procedure impiegati, di informazioni concernenti una persona fisica identificata o identificabile

  Esempi: Upload immagine in ChatBot, analisi immagine tramite software, iscrizione nella cartella del paziente di informazioni fornite dall'IA, **profilazione** ai fini di predizione dello stato di salute ecc.

- Dati ordinari vs dati personali degni/meritevoli di particolare protezione (→ **consenso espresso**, **rischi e sicurezza**)

- Principi del trattamento (ad es. liceità, minimizzazione della lesione, qualità dei dati personali)

- Obblighi del titolare e/o del responsabile dell'elaborazione (ad es. (i) informare, (ii) diligenza in materia di sicurezza, (iii) DPA, (iv) divieto di trasferimento all'estero, (v) base legale (LPDP), (vi) notifica delle violazioni e (vii) VIPD)

AGENDA

4. Segreto professionale e segreto d’ufficio

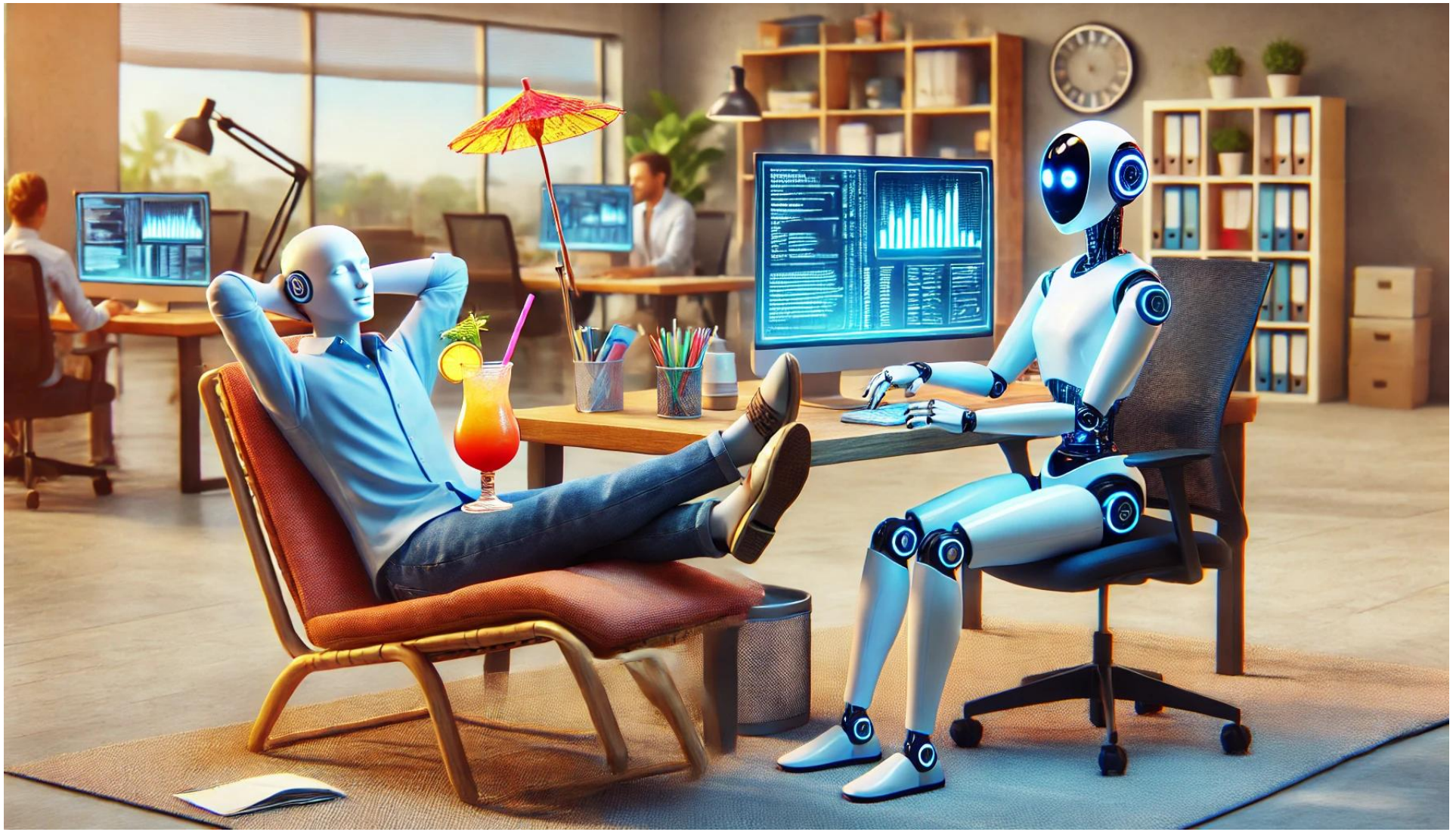
- Violazione della **confidenzialità** dei dati
  - Commissione
  - **Omissione**: mancata adozione di misure di protezione!
- Consenso informato quale "panacea"?
- Impresa "IA" "**ausiliario**" del professionista / autorità o funzionario astretto al segreto?
  - ✓ se il fornitore è consapevole del suo ruolo e **"assume" tali obblighi**!
- Nessuna "impossibilità giuridica"
- De facto? Risoluzione privatim 24.11.25 sul Cloud

L'utilisation de solutions SaaS internationales pour des données personnelles sensibles ou soumises à une obligation légale de garder le secret par des organes publics est possible uniquement si les données sont cryptées par l'organe responsable lui-même et que le fournisseur de services de cloud computing n'a pas accès à la clé.

AGENDA

5. Aspetti delicati e rischi; obblighi del titolare dell'elaborazione

- «Shadow AI», «Shadow data subject»
- «Supply chain» sconosciuta e incontrollata 
- Trattamenti illeciti di dati personali (elaborazioni, profilazioni, processi decisionali) 
- Consensi insufficienti
- Trasparenza insufficiente 
- Violazione dell'obbligo di garanzia di sicurezza 
- Trasmissioni di dati personali verso Stati inadeguati 
- Perdita di controllo sul fornitore (DPA) 
- Ruoli e responsabilità non chiari; Carenza di direttive e istruzioni interne
- La conformità non è «documentata» (DL LPDP)
- Delega «selvaggia» / Abdicazione di ruolo (inclusi i «Capi»)
- Carenza di competenze e sensibilizzazione insufficiente del personale
    - Perdita dello spirito critico da parte dell'utente
    - Deresponsabilizzazione / Sensazione di impunità dell'utente



AI chatbots can be tricked by hackers into stealing your data



Graham CLULEY
October 22, 2024

Promo Protect all your devices, without slowing them down.
Free 30-day trial

Security researchers have uncovered a new flaw in some AI chatbots that could have allowed hackers to steal personal information from users.

A group of researchers from the University of California, San Diego (UCSD) and Nanyang Technological University in Singapore discovered the flaw, which they have nameed "Imprompter", which uses a clever trick to hide malicious instructions within seemingly-random text.

https://www.axios.com/2024/04/03/ai-chatbots-def-con-red-team-hack

https://www.bitdefender.com/en-us/blog/hotforsecurity/ai-chatbots-can-be-tricked-by-hackers-into-stealing-your-data

https://www.gov.uk/government/publications/research-on-the-cyber-security-of-ai/cyber-security-risks-to-artificial-intelligence#list-of-case-studies

- Obbligo di **informazione** del paziente
- Obbligo di svolgere una **valutazione d'impatto** sulla protezione dei dati personali (DPIA) e di consultazione preventiva dell'autorità di vigilanza competente
- Obbligo di concludere un contratto con il fornitore (DPA) che disciplini l'elaborazione dei dati personali e vincoli l'intera "supply chain"; scelta, istruzione e sorveglianza efficace del processor!
  - *Il titolare del trattamento deve garantire che il responsabile del trattamento rispetti la legge in misura uguale a lui. Ciò riguarda in particolare il rispetto dei principi generali, delle regole relative alla sicurezza dei dati, espressamente menzionate nel capoverso 2, e delle regole relative alla comunicazione all'estero.*
  - *Il titolare del trattamento deve impedire le violazioni della legge.*
  - *Deve scegliere con cura il responsabile del trattamento, istruirlo in modo adeguato e sorvegliarlo nella misura del necessari*
  - Direttive privatim per servizi Cloud nel settore pubblico 14 febbraio 2022 (link)
  - Base legale per i trattamenti sistematici di dati personali nel settore pubblico?

- Obbligo di garantire, mediante appropriati provvedimenti tecnici e organizzativi, che la sicurezza dei dati personali sia adeguata al rischio
  - Confidenzialità, integrità, disponibilità dei dati e tracciabilità delle attività di trattamento
  - Standard minimi di sicurezza (art. 1 – 6 OPDa)
  - Linee Guida IFPDT:
    - Guida ai provvedimenti tecnici e organizzativi concernenti la protezione dei dati (TOM) (LINK)
    - Raccomandazioni tecniche dell'IFPDT per la verbalizzazione secondo l'articolo 4 OPDa (15 settembre 2023) (LINK)
  - B/HYOK: dati sensibili (medici) e segreti (Cloud)
  - Autenticazione sicura e accesso ai servizi IA su base di necessità
  - Obbligo di selezionare, istruire e sorvegliare i dipendenti

AGENDA

6. Le decisioni individuali automatizzate

- Decisione basata esclusivamente su un trattamento di dati personali automatizzato che determina effetti giuridici o conseguenze significative
  - LPDP: consenso «espresso» ove necessario
  - Obbligo di informazione (salvo eccezioni)
  - Diritto di esprimersi (su richiesta)
  - Diritto al riesame da parte di una persona fisica
- Esempi:
  - Analisi di immagini basata su IA non verificata da una persona umana che determina conseguenze per il paziente
  - Profilazione dei pazienti sulla base di algoritmi predittivi + conseguenze per il paziente

AGENDA

7. Bonus Track: Principali quesiti da porsi

- Vi è una strategia di implementazione dell'IA chiara adottata dall'organo competente?
- Il principio di liceità è rispettato?
- Una valutazione d'impatto sulla protezione dei dati (DPIA) è necessaria?
- Disponiamo di contrattualistica adeguata con il fornitore di servizi IA (DPA, NDA, ecc.)? Qual è la supply chain?
- Adempiamo all'obbligo di informare le persone interessate relativamente all'uso che facciamo dei loro dati personali?
- Disponiamo di misure per verificare l'attendibilità / assenza di bias degli output generati?
- Vi sono trasferimenti di dati verso Stati non adeguati?
- In caso di decisioni automatizzate disponiamo di procedure che permettano alle persone di esprimere un parere o di fare riesaminare la decisione da un essere umano?
- Il sistema IA è adeguatamente protetto contro violazioni di dati personali, abusi e altri attacchi alla sicurezza?
- Siamo in grado di garantire i diritti d'accesso, rettifica e cancellazione dei dati degli utenti?
- I collaboratori sono correttamente scelti, istruiti e sorvegliati?
- L'uso di strumenti privati (App e dispositivi) è adeguatamente gestito?

Siti istituzionali

- https://www.edoeb.admin.ch/edoeb/it/home.html (incaricato federale)
- https://www4.ti.ch/can/sgcds/pd/generalita (incaricato cantonale ticinese)
- https://swissprivacy.law/ (raccolta di articoli e dottrina)

Letture raccomandate:

- La nuova legge sulla protezione dei dati dal punto di vista dell'IFPDT (IFPDT)
- La nouvelle loi sur la protection des données (Rosenthal)
- La (nouvelle) Loi fédérale sur la protection des données du 25 septembre 2020 : des principes, des droits et des obligations (Métille)

GRAZIE!

Avv. Gianni CATTANEO, LL.M.

www.cbm-lex.ch

gianni.cattaneo@cbm-lex.ch