Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
Préposé fédéral à la protection des données et à la transparence PFPDT
Incaricato federale della protezione dei dati e della trasparenza IFPDT
Incumbensà federal per la protecziun da datas e per la transparenza IFPDT

privatim
Konferenz der schweizerischen Datenschutzbeauftragten
Conférence des préposé(e)s suisses à la protection des données
Conferenza degli incaricati svizzeri per la protezione dei dati

Promemoria

Sorveglianza di persone assistite

Trattamento dei dati tramite telecamere e altri sensori impiegati in ospedali, case di cura e istituti simili

La sorveglianza digitale delle persone assistite in ospedali, case di cura e istituti simili sta acquisendo sempre maggiore importanza in ragione dello sviluppo tecnologico e del gran numero delle relative offerte di prodotti e servizi. A seconda del diritto applicabile nel caso specifico, il trattamento dei dati personali da parte di tali strutture può rientrare nelle competenze di vigilanza dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) o delle autorità cantonali di protezione dei dati. Per questo motivo, l'IFPDT e la Conferenza degli incaricati svizzeri per la protezione dei dati (privatim) hanno ritenuto opportuno pubblicare congiuntamente il presente promemoria, al fine di sensibilizzare i titolari del trattamento alle sfide in materia di protezione dei dati derivate dall'impiego di sistemi di sorveglianza. Si noti che la presente pubblicazione si concentra unicamente sulla sorveglianza delle persone assistite e non tratta quindi la sorveglianza più generale della struttura, ossia le telecamere posizionate in corridoi, ingressi, sale d'attesa ecc.

I. Osservazioni preliminari

Le soluzioni di sorveglianza e assistenza digitali (guida assistita, sicurezza, giocattoli, ecc.) si stanno diffondendo in tutti i settori. Il mercato propone sempre più prodotti multimodali con varie funzionalità (p. es. rilevamento di movimento e di presenza, tracciamento oculare, comunicazione diretta spesso abbinata all'intelligenza artificiale) basate su tecnologie come le telecamere ottiche, i microfoni, i radar o i sensori a infrarossi. Spesso questi sistemi non si limitano a registrare dei dati (immagini, audio, dati radar ecc.), bensì li analizzano in modo più o meno approfondito; rilevano automaticamente anomalie e innescano allarmi, permettendo un intervento (umano o algoritmico, preventivo o reattivo) sul campo. Questo contesto sta evolvendo rapidamente e a medio termine si prevede che le soluzioni proposte dai fornitori risulteranno sempre più globali, combinando quindi diverse tecnologie e offrendo capacità d'utilizzo molto ampie che vanno oltre le reali esigenze dell'utilizzatore. Il presente promemoria si inserisce in questa dinamica e affronta il tema della sorveglianza nell'ambito delle cure. Non presenta in dettaglio tutte le tecnologie attualmente disponibili sul mercato o le loro eventuali combinazioni, bensì si concentra su alcune di esse al fine di illustrare le sfide e identificare i punti rilevanti. Ciononostante, i principi discussi di seguito si applicano in modo generale a prescindere dalle tecnologie e soluzioni impiegate.

Sebbene la sorveglianza digitale nell'ambito delle cure sollevi anche questioni legate a diversi altri contesti, in particolare per quanto riguarda il diritto del lavoro e della sanità pubblica o l'etica, il presente documento si concentra sulla protezione dei dati.

In generale, questo tipo di sorveglianza corrisponde a un trattamento di intensità elevata poiché viola la sfera privata e persino intima delle persone assistite, le quali si trovano spesso in situazioni di vulnerabilità. Nel caso dei soggiorni prolungati si aggiunge il fatto che

la sorveglianza può essere considerata come effettuata presso il «domicilio» delle persone interessate.

Anche se l'intensità del trattamento può variare in base alla situazione e alle tecnologie impiegate, i principi che regolano l'attuazione delle misure nonché le questioni relative alla protezione dei dati sono generalmente gli stessi.

II. Aspetti relativi alle tecnologie

Il presente documento descrive dapprima il funzionamento di determinate tecnologie e in seguito esamina le relative questioni giuridiche.

1. Sensori ottici

Al fine di illustrare alcune sfide tecnologiche, sarà prima di tutto presentato il concetto di sorveglianza ottica e in seguito l'analisi sarà estesa anche ad altre tecnologie. Di seguito sono descritti brevemente i diversi tipi di sorveglianza ottica.

- **Sorveglianza analogica diretta**: l'assistente è seduto su una sedia posizionata nella stanza della persona assistita.

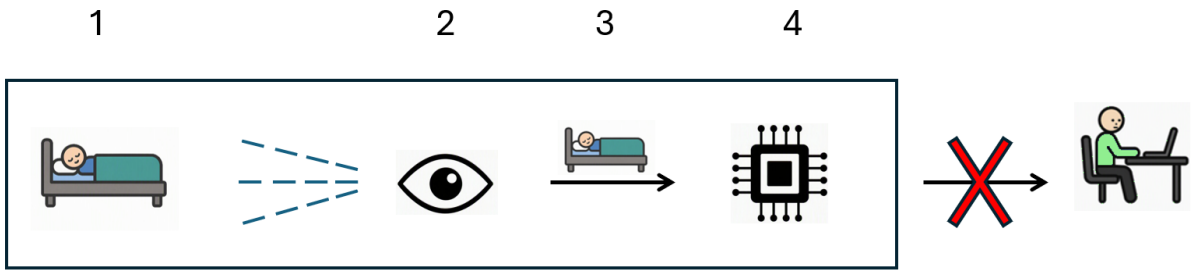
- **Sorveglianza diretta digitale**: una telecamera installata all'interno della stanza proietta l'immagine in tempo reale su uno schermo controllato dall'assistente.

- **Sorveglianza indiretta digitale**: una telecamera e un'unità informatica sono installate nella stessa stanza. La telecamera trasmette l'immagine all'unità, che la converte in un pittogramma corrispondente alla posizione o al comportamento della persona assistita (sdraiata, per terra, seduta, in piedi, agitata, ecc.). Il pittogramma è poi proiettato in tempo reale sullo schermo dell'assistente. L'elemento indiretto consiste nella tappa intermedia, ossia il trattamento dei dati grezzi da parte dell'unità informatica, che li converte in dati elaborati prima di trasmetterli all'assistente.

- **Sorveglianza digitale indiretta situazionale**: caso analogo al precedente, con la differenza che l'assistente viene informato solo se è stata rilevata una situazione predefinita (p. es. caduta). In questo caso l'unità informatica trasmette un segnale d'allarme ed eventualmente converte l'immagine in un pittogramma che è proiettato sullo schermo. Questo tipo di sorveglianza è definita situazionale poiché i dati elaborati sono trasmessi all'assistente solo in determinate situazioni.

I paragrafi successivi si concentrano su quest'ultimo tipo di sorveglianza: da un lato, il suo valore didattico consente di affrontare diversi punti centrali legati all'uso delle diverse tecnologie; dall'altro, questo tema solleva numerose riflessioni.

La sorveglianza digitale indiretta situazionale può essere schematizzata in questo modo:



Legenda:

1: oggetto della sorveglianza, ossia la persona assistita nel suo letto all'interno dell'istituto

2: sensore, ossia una telecamera ottica

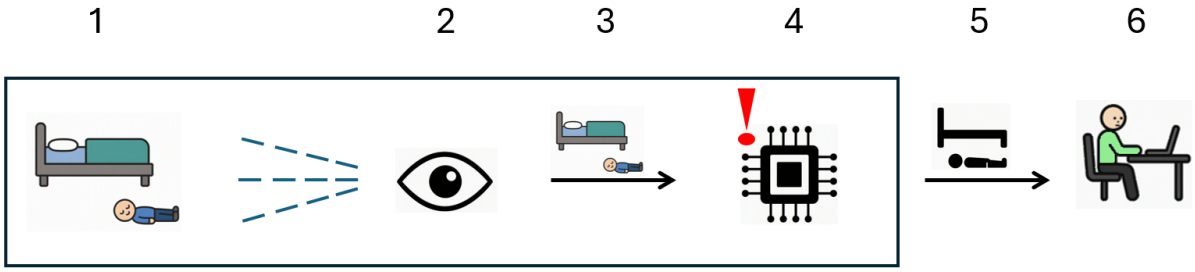
3: dati grezzi, ossia l'immagine registrata dal sensore e trasmessa all'unità informatica

4: unità informatica installata nella stanza (o nell'alloggiamento del sensore) che identifica la situazione particolare, trasmette il segnale d'allarme e se del caso converte l'immagine in un pittogramma

L'intero processo avviene all'interno della stanza (rappresentata qui dalla cornice nera).

Il sensore (in questo caso una telecamera) registra un'immagine e la trasmette all'unità informatica per il trattamento (identificazione di una situazione particolare). Nello schema precedente nessun dato lascia la stanza per essere trasmesso allo schermo, poiché la situazione è «sotto controllo» (la persona dorme nel suo letto).

In caso di caduta, lo schema appare invece come segue:



L'unità informatica ha rilevato una caduta. Viene trasmesso un segnale d'allarme e l'immagine è convertita in un pittogramma (5) e proiettata sullo schermo dell'assistente (6) o su un apparecchio analogo, per esempio un cercapersone o un tablet.

Questo secondo esempio illustra il principio della minimizzazione dei dati (cfr. n. III. 4). Per rilevare cadute o altri incidenti non è necessario avere accesso all'immagine vera e propria. Il filtraggio eseguito dall'unità informatica consente di trasmettere all'assistente solo i dati strettamente necessari, ossia dati elaborati come un segnale d'allarme o un pittogramma, ed esclusivamente in situazioni predefinite. Finché la situazione non risulta particolare, nessun dato grezzo o elaborato lascia la stanza.

2. Altre tipologie di sensori e scelta della tecnologia

Come accennato, la sorveglianza indiretta nell'ambito delle cure può avvenire anche tramite altre tecnologie quali le telecamere a infrarossi o i radar.

Le telecamere a infrarossi rilevano le differenze di temperatura e generano delle sagome in corrispondenza di oggetti e persone presenti all'interno della stanza. I radar invece misurano la distanza degli elementi rispetto al trasmettitore, tracciando un rilievo degli oggetti e delle persone e rilevando i movimenti.

A dipendenza del sensore utilizzato (ottico, termico o radar), i dati grezzi raccolti non sono gli stessi e possono fornire informazioni differenti. Al contrario della telecamera ottica, i sensori termici e i radar non generano immagini fotografiche, ma possono raccogliere altri tipi di dati che una telecamera non è in grado di rilevare. Misurando la temperatura corporea della persona assistita, i sensori a infrarossi possono fornire informazioni aggiuntive sul suo stato (febbre, stress, ecc.). I radar rilevano invece elementi come il ritmo cardiaco e respiratorio. Si noti inoltre che il sistema di sorveglianza è obbligatoriamente associato a una stanza o a un letto, affinché l'assistente sappia dove recarsi in caso d'allarme. Le stanze o i letti sono anch'essi associati a una persona (eventualmente in un sistema d'informazione diverso da quello a cui è associato il dispositivo di sorveglianza). Pertanto, sebbene i dati grezzi di radar e infrarossi non permettano d'identificare direttamente una persona, non si tratta propriamente di anonimato bensì di pseudonimizzazione.

Infine, anche la risoluzione del sensore riveste un ruolo importante: a parità di condizioni (campo visivo della telecamera, zoom ottico, ecc.), una telecamera da 0,5 megapixel registra meno informazioni rispetto a una da 10 megapixel. Ciò vale ovviamente per tutte le tecnologie prese in considerazione.

Le sfide legate alla scelta della tecnologia di sorveglianza sono affrontate al numero III. 5.

III. Aspetti giuridici

1. Diritto applicabile in materia di protezione dei dati

È innanzitutto necessario fare una distinzione in merito alla qualità dell'istituto di cura interessato: gli organi pubblici[1] (in linea di principio cantonali, dato che la sanità è competenza dei Cantoni) sono soggetti al principio di legalità e al diritto cantonale in materia

[1] Si ricorda che questa qualifica non dipende dalla forma giuridica dell'istituto, bensì dal suo mandato. Per esempio, una clinica privata che effettua interventi ortopedici su mandato cantonale è considerata come un organo pubblico. Si noti inoltre che uno stesso istituto può essere considerato come un organo pubblico per alcune delle proprie attività (quelle coperte dal mandato cantonale) e come privato per le altre.

di protezione dei dati, mentre gli istituti privati sono soggetti alla legge federale sulla protezione dei dati e non si applica il principio di legalità.

Tuttavia, al di là della questione della base giuridica, i principi che regolano l'attuazione delle misure di sorveglianza sono essenzialmente gli stessi e sono presenti sia nelle leggi cantonali che nella legge federale. Le pagine seguenti illustrano quelli fondamentali che vanno rispettati.

2. Legittimità del trattamento e consenso

Ogni trattamento dei dati deve essere lecito. Come accennato, questo concetto è valutato diversamente a seconda del tipo di istituto (pubblico o privato).

Per gli enti pubblici vale il principio di legalità, secondo il quale tali enti devono disporre di una base giuridica per le loro azioni. Un ente pubblico può quindi trattare dati personali solo se esiste una base giuridica a tal fine. La sorveglianza deve pertanto essere indispensabile per l'adempimento di un compito previsto dalla legge oppure essere espressamente prevista da una legge. La sorveglianza di un paziente nell'ambito del piano terapeutico può, ad esempio, basarsi sul mandato di assistenza previsto dalla legge. Il consenso non può sostituire la base giuridica richiesta dal principio di legalità. A ciò si aggiunge il fatto che gli enti pubblici svolgono il loro mandato assistenziale in modo indipendente.

Gli istituti privati sono soggetti alla legge federale sulla protezione dei dati (LPD). Secondo l'articolo 30 capoverso 1 LPD, un trattamento dei dati non può ledere illecitamente la personalità delle persone interessate. Il capoverso 2 precisa che vi è lesione della personalità in particolare se sono trattati dati personali in violazione dei principi di cui agli articoli 6 e 8 LPD o contro l'espressa volontà della persona interessata, o ancora se sono comunicati a terzi dati personali degni di particolare protezione. Se un trattamento lede illecitamente la personalità, è necessario verificare se esiste un motivo giustificativo (art. 31 LPD). Nel contesto in esame, possono essere presi in considerazione essenzialmente il consenso della persona interessata e un interesse privato preponderante.

Tra i tre casi «classici» dell'articolo 30 capoverso 2 LPD, la comunicazione di dati a terzi non si applica a priori a questo contesto, dato che il sistema di sorveglianza è impiegato unicamente a fini interni. La questione dell'opposizione della persona assistita sarà approfondita ulteriormente. Per quanto riguarda i principi fondamentali (in particolare quello della finalità, della riconoscibilità e della proporzionalità), non è escluso che possano essere rispettati[2], se la persona assistita è capace di discernimento e il suo stato psicofisico le permette effettivamente di far valere i propri diritti senza ambiguità (in particolare il diritto all'opposizione; cfr. più in basso). In una situazione del genere dove la persona assistita non presenta vulnerabilità particolari, la sorveglianza non costituisce necessariamente una

[2] Questo potrebbe essere il caso se i dati sono trattati per uno scopo preciso, la persona assistita è stata adeguatamente informata e il principio della proporzionalità è rispettato. Questi aspetti sono esaminati più nel dettaglio in seguito.

lesione della personalità e di conseguenza non è richiesto un motivo giustificativo ai sensi dell'articolo 31 LPD.

Si invita tuttavia alla prudenza. Prima di tutto, l'elenco delle ipotesi presentato all'articolo 30 capoverso 2 non è esaustivo, come mostra la locuzione «in particolare». Sono quindi ipotizzabili altre situazioni che comportano una lesione della personalità, soprattutto in un ambito sensibile e intimo come quello in questione. A ciò si aggiunge il fatto che gli istituti di cura responsabili non possono impostare le misure di sorveglianza basandosi su persone nel pieno delle loro facoltà se queste non sono rappresentative dell'istituto in questione.

Inoltre, se si dovesse ritenere che non vi è alcuna lesione della personalità, ciò significherebbe che non è necessario un motivo giustificativo e a maggior ragione nemmeno il consenso. Questa affermazione fa sorgere diverse osservazioni.

Tra i diversi principi della LPD figura anche quello della riconoscibilità (art. 6 cpv. 3 LPD), concretizzato dall'obbligo d'informare (art. 19 LPD). Secondo l'articolo 19, il titolare deve informare la persona interessata, specialmente in merito alla raccolta dei dati e allo scopo di tale operazione. Più i dati sono sensibili e la situazione «delicata», più le informazioni dovranno essere comunicate in modo completo e attivo. Nell'ambito in esame, alla luce dell'intensità dal trattamento dei dati, sarebbe opportuno che il personale fornisca e spieghi personalmente le informazioni alla persona assistita; una semplice scheda informativa non è sufficiente. Di conseguenza, tenuto conto di questo obbligo d'informare «rafforzato», si può affermare che l'atto di richiedere l'espresso consenso (art. 6 cpv. 7 LPD), oltre alla «semplice» informazione della persona assistita, non rappresenta un carico aggiuntivo significativo per l'istituzione (l'informazione è del resto un elemento necessario per il consenso – art. 6 cpv. 6 LPD). Sembra quindi opportuno richiedere sempre il consenso quando possibile, a maggior ragione se si considera il rapporto di fiducia tra la persona assistita e l'assistente.

Detto ciò, l'altra condizione del consenso è la sua natura libera e a tal proposito la situazione risulta delicata. La persona assistita si trova spesso in una situazione di vulnerabilità. Inoltre, può percepire della pressione (anche involontaria) da parte dell'istituto in cui soggiorna. Il consenso non è quindi una soluzione adeguata in tutti i casi.

Analogamente, la persona assistita non si sentirà necessariamente in condizione di esercitare il suo diritto d'opposizione, anche se prova disagio all'idea di essere osservata. Di conseguenza, non è sempre possibile definire un trattamento come lecito solo perché rispetta i principi della LPD e la persona assistita non vi si è opposta.

Inoltre, nel caso delle persone assistite incapaci di discernimento tale consenso non può comunque essere ottenuto: considerato il carattere intimo del trattamento dei dati (nel luogo di residenza della persona), non sembra infatti possibile richiederlo tramite rappresentanza (a meno che non si consideri la sorveglianza come un atto medico, nel qual caso si può richiedere il consenso ai familiari).

In conclusione, sia le soluzioni di consenso («opt-in») che d'opposizione («opt-out») non risultano sufficienti per legittimare una sorveglianza, anche se è comunque opportuno

richiedere sempre il consenso quando possibile. Se un istituto desidera installare delle misure di sorveglianza, deve quindi poterlo giustificare con un interesse preponderante. Sebbene l'articolo 31 capoverso 1 LPD menzioni unicamente l'interesse preponderante del titolare del trattamento, si riconosce che tale interesse può anche corrispondere a quello della persona interessata, soprattutto nell'ambito delle cure. Pertanto, qualsiasi sistema di sorveglianza deve avere come obiettivo principale il miglioramento dell'assistenza del paziente[3]. Questo argomento sarà approfondito nel prossimo capitolo.

3. Principio della finalità

Questo principio prevede che i dati siano trattati unicamente per uno scopo preciso, compatibile con le informazioni fornite al momento della raccolta dei dati. Prima di installare un sistema di sorveglianza, l'istituto interessato deve quindi definire in modo chiaro i propri obiettivi. Come già accennato, essi devono prima di tutto servire l'interesse della persona assistita e prevalere su qualsiasi potenziale violazione della sua personalità. In quest'ottica, considerata l'intensità del trattamento dei dati derivata da queste misure di sorveglianza, l'ottimizzazione di processi logistici e organizzativi (p. es. sapere se un letto è fatto o un pasto è finito) non è un motivo sufficiente. Inoltre, gli obiettivi devono essere perseguiti in un caso concreto: non si può installare sistematicamente un sistema di sorveglianza senza tenere conto della situazione particolare della persona assistita. A maggior ragione bisogna evitare che queste misure riducano la qualità dell'assistenza (p. es. il sistema di sorveglianza induce gli assistenti a recarsi meno frequentemente nella stanza della persona assistita, con conseguenti effetti negativi sul suo stato di salute mentale).

Anche gli enti pubblici sono tenuti a rispettare il principio di finalità. Pertanto, anch'essi devono definire chiaramente, già prima dell'utilizzo dei sistemi di sorveglianza, a quali fini debba essere effettuata la sorveglianza. Tuttavia, possono essere perseguiti solo obiettivi che siano coperti dalla base giuridica. In tal senso, i fini ammissibili sono limitati dalle rispettive basi giuridiche.

4. Principio della proporzionalità

Di fondamentale importanza, il principio della proporzionalità prevede di trattare unicamente i dati necessari al raggiungimento dell'obiettivo prefissato. Si suddivide in tre elementi:

- idoneità: la misura impiegata deve consentire di raggiungere l'obiettivo;
- necessità: si deve scegliere la misura meno incisiva;
- proporzionalità in senso stretto: deve esistere un rapporto ragionevole tra l'obiettivo e l'intensità del trattamento dei dati.

Nella pratica, questo implica sempre una ponderazione tra l'intensità del trattamento dei dati (sorveglianza costante, durata prolungata, carattere intrusivo, immagini ad alta definizione,

[3] Possono potenzialmente essere presi in considerazione anche altri interessi (p. es. la sicurezza del personale o di altri pazienti); questa questione non sarà però approfondita nel presente documento, che si concentra sull'assistenza della persona che riceve le cure.

sorveglianza in tempo reale, audio, combinazione di diversi sistemi di sorveglianza, ecc.) e la sua efficacia. Maggiore è l'intensità, maggiore deve essere la sua efficacia e più importante deve essere l'obiettivo perseguito. Come già indicato nella sezione «Principio della finalità», dei semplici miglioramenti organizzativi non sono un motivo sufficiente.

Oltre al tipo di sorveglianza impiegata, si deve tenere conto anche di diversi altri fattori, illustrati qui di seguito.

- **Minimizzazione dei dati**: è importante ridurre il più possibile la quantità dei dati trattati. Sono quindi da privilegiare le soluzioni di sorveglianza indiretta esposte al numero II.
- **Opzioni di configurazione**: le capacità della soluzione proposta possono superare le necessità del caso specifico (zoom, registrazione audio, qualità dei dati grezzi ecc.). Se non è possibile rinunciare alla soluzione in favore di una più semplice (p. es. le funzioni supplementari sono richieste per determinate situazioni), è importante avere la possibilità di configurare il sistema e disattivare le funzioni non necessarie, così da evitare di generare dati superflui.
- **Conservazione dei dati**: conservare dati grezzi o elaborati per un periodo più o meno prolungato genera rischi considerevoli. In linea di principio, nel contesto della sorveglianza nell'ambito delle cure non è giustificato conservare i dati oltre la durata tecnica del trattamento (tempo che i processi informatici impiegano per trattare i dati e trasmetterli). In ogni caso, un'eventuale conservazione deve conseguire un obiettivo concreto e legittimo; delle semplici questioni di praticità non sono sufficienti.
- **Limitazioni del caso specifico**: la sorveglianza non deve essere applicata in modo sistematico a tutte le persone assistite; ogni misura deve essere giustificata individualmente e rivalutata a cadenza regolare.
- **Integrazione in una rete**: l'accessibilità di un sistema tramite una rete (interna o esterna) e più in generale la sua integrazione in una rete aumenta considerevolmente il rischio di errori o di attacchi informatici. È quindi necessario limitare il più possibile questi fattori o rinunciarvi. Gli accessi al sistema devono essere stabiliti in modo coerente e limitati a una cerchia ristretta.

Esempi di situazioni:

- **Rilevatore di cadute all'interno della stanza**: deve essere possibile disattivare il dispositivo tramite un interruttore posto nella stanza, in particolare durante le visite di assistenti o familiari. Considerato il suo scopo, in tali situazioni non è giustificato mantenerlo in funzione.
- **Allarme in caso d'incidente**: se il sistema è pensato per rilevare incidenti particolari come le cadute, non è necessario trasmettere immagini ad alta definizione agli assistenti (fanno eccezione le esigenze specifiche legate alla terapia intensiva e alle cure acute). Nella maggior parte dei casi è sufficiente un allarme sonoro o visivo (cfr. anche n. II).
- **Prevenzione delle cadute dal letto**: a seconda della valutazione medica e del caso specifico, le barriere retrattili possono costituire un'alternativa ai sensori.

5. Scelta della tecnologia

Nell'ambito di una sorveglianza digitale indiretta (situazionale), la scelta della tecnologia solleva diverse questioni particolari. Il trattamento dei dati avviene in due fasi, ossia la registrazione dei dati grezzi e la successiva trasmissione dei dati elaborati. In linea di massima, i dati grezzi non devono essere accessibili e servono unicamente per essere convertiti in dati elaborati. Non hanno altra utilità e non sono destinati ad altri scopi. I dati elaborati sono invece modellati in base alle necessità (pittogrammi o allarmi) e ognuna delle tecnologie menzionate precedentemente (sensore ottico o a infrarossi, radar) è in grado di generarne di simili.

Pertanto, la scelta della tecnologia non è determinante dal punto di vista delle esigenze dell'istituto, poiché ogni sistema può offrire prestazioni simili[4]. Ciò merita alcune osservazioni.

Il diritto federale in materia di protezione dei dati prevede il principio della protezione fin dalla progettazione («privacy by design»). Esso non è citato esplicitamente nelle leggi cantonali; tuttavia, gli incaricati cantonali sono consultati regolarmente se non perfino coinvolti nello sviluppo dei progetti, di modo che questo principio è comunque rispettato. Inoltre, si sovrappone parzialmente con il principio della sicurezza dei dati previsto dalle leggi cantonali (cfr. più avanti). Quello della «privacy by design» è un principio trasversale che impone ai titolari del trattamento di sviluppare una soluzione per il trattamento che rispetti la protezione dei dati, in particolare per quanto riguarda i principi menzionati precedentemente. In questo senso, è anche un modo per attuare il principio della proporzionalità.

Inoltre, i titolari del trattamento devono scegliere soluzioni e tecnologie adatte per quanto riguarda lo stato della tecnica, la natura, portata e scopo del trattamento nonché i rischi per la personalità o per i diritti fondamentali delle persone interessate. Questo vale anche per i dati grezzi, che presentano delle differenze qualitative e quantitative a seconda della tecnologia impiegata. Si rinvia in tal senso alla parte tecnica del presente documento, dove sono espresse considerazioni in merito alle capacità e ai rischi di ciascuna tecnologia (n. II). In questo contesto, per quanto riguarda la natura dei dati trattati e la portata del trattamento, la valutazione dell'adeguatezza avviene sempre facendo riferimento a un obiettivo concreto[5]. La tecnologia scelta deve garantire un livello di affidabilità sufficiente al raggiungimento dell'obiettivo prefissato (attivare un allarme quando necessario) e al contempo permettere di limitare i falsi positivi, poiché ogni falso allarme comporta un

[4] Si considerano qui le situazioni «semplici» dove vengono generati dei pittogrammi o un segnale d'allarme in caso di cadute o di altri comportamenti anomali. A seconda della tecnologia è possibile monitorare parametri come la temperatura o il ritmo cardiaco. Se l'istituto di cura è interessato a tali parametri, questa necessità può orientare la scelta verso una tecnologia in particolare – tenendo presente che esistono anche altri strumenti per il monitoraggio (p. es. termometro o cardiofrequenzimetro posizionato sul polso).

[5] Telecamera ottica in tempo reale: questa soluzione potrebbe essere giustificata in un reparto di terapia intensiva, dato che risponde a un'esigenza clinica chiaramente definita e che la configurazione dei reparti impedisce al personale di avere una visione d'insieme sui diversi pazienti.

intervento da parte del personale e potenzialmente una violazione ingiustificata della sfera privata della persona assistita. Al contempo, nella valutazione complessiva possono essere presi in considerazione anche vincoli di tipo organizzativo e finanziario, che tuttavia non devono prevalere sull'obbligo di tutelare i diritti fondamentali delle persone. In tal senso, è necessario tenere conto anche delle misure adottate per gestire eventuali conseguenze negative o rischi legati a determinate scelte (p. es. di natura tecnologica). L'adeguatezza di una soluzione deve quindi essere valutata nel suo insieme e sulla base del contesto.

Inoltre, sia il diritto federale in materia di protezione dei dati che i diritti cantonali prevedono il principio della sicurezza dei dati. Nel contesto del presente documento, questo si traduce in misure concrete per garantire che non sia effettivamente possibile accedere ai dati grezzi, nemmeno durante i periodi di manutenzione e di aggiornamento dei software (fanno eccezione gli accessi per motivi tecnici, dove è consentita una connessione fisica diretta con il sensore al fine di verificarne il funzionamento). I titolari del trattamento devono essere in grado di presentare prove in tal senso in ogni momento, facendo riferimento a descrizioni sufficientemente dettagliate del produttore e, se del caso, documentando le proprie verifiche supplementari (per ulteriori informazioni sull'obbligo di documentazione, cfr. n. IV). In caso contrario, l'impiego dei sensori di sorveglianza in questione è considerato illecito, a prescindere dal tipo di tecnologia (ottica, a infrarossi, radar). Nemmeno il consenso della persona interessata o interessi privati o pubblici preponderanti sono una giustificazione valida.

In conclusione, gli istituti dispongono di un margine di manovra nella scelta delle tecnologie e delle funzionalità, che tuttavia incidono sull'intensità del trattamento e della sorveglianza. I principi della «privacy by design» e della sicurezza dei dati impongono di giustificare e documentare le scelte in relazione agli obiettivi prefissati e alle limitazioni di attuazione. Nella pratica, se un istituto di cura intende adottare una soluzione di questo tipo, il progetto deve essere gestito con attenzione sin dall'inizio. Il responsabile del progetto deve coinvolgere le figure chiave (consulenti per la protezione dei dati, servizio giuridico, dirigenti, tecnici, assistenti, ecc.) già dalle prime riflessioni, scegliere il prodotto adatto alla situazione e svolgere una valutazione dei rischi sistematici e specifici per ognuna delle opzioni disponibili, verificandone le possibilità di configurazione. Non deve fare affidamento esclusivamente sulla documentazione commerciale bensì richiedere al fornitore le informazioni tecniche necessarie a documentare i trattamenti nonché a identificare i rischi e le misure per limitarli. Il responsabile del progetto è tenuto a informare in modo trasparente i dirigenti in merito ai rischi residui, così da permettergli di prendere decisioni con cognizione di causa. L'istituto di cura deve verificare la conformità del prodotto prima dell'acquisto, al momento dell'implementazione e in modo continuativo anche in seguito.

6. Chilling effect

Dal punto di vista della proporzionalità, bisogna anche tenere conto del potenziale effetto dissuasivo («chilling effect») di questi dispositivi di sorveglianza, poiché la semplice consapevolezza che ne è stato installato uno può modificare il comportamento delle persone interessate.

Si pensi innanzitutto alla persona assistita: anche se il sistema è giustificato e sono state fornite informazioni adeguate in merito al funzionamento e ai limiti del dispositivo, il pensiero

di essere osservati può causare disagio e influenzare il comportamento della persona. Questo può valere anche nel caso di assistenti e visitatori, fintanto che il sistema rimane attivo in loro presenza. Tale effetto dissuasivo può avere un impatto particolarmente negativo sugli assistenti poiché potrebbe influenzare il loro comportamento e di conseguenza la qualità delle cure.

7. Intelligenza artificiale

L'intelligenza artificiale (IA) è sempre più utilizzata in questo contesto. Nell'ambito delle soluzioni di sorveglianza indirette, il trattamento preliminare da parte dell'IA può permettere di ridurre la quantità di dati che lasciano la stanza e quindi delle informazioni trasmesse agli assistenti (un semplice pittogramma o un segnale d'allarme).

Nonostante i vantaggi, l'utilizzo dell'IA comporta anche problematiche e rischi. Si pensi per prima cosa al luogo del trattamento dei dati: nel limite del possibile, l'IA deve effettuare il trattamento localmente, ossia nella stanza della persona assistita. Ricorrere a soluzioni cloud risulta delicato, in quanto esse comportano rischi specifici legati soprattutto all'accessibilità dei dati (in particolare da parte del fornitore di cloud). Bisognerebbe pertanto dimostrare che non è possibile impiegare delle soluzioni locali (p. es. per motivi di complessità e costi) e chiarire in che modo può essere garantito il rispetto dei principi della proporzionalità, della sicurezza e della «privacy by design». È problematico anche il riutilizzo dei dati ai fini dell'addestramento dei modelli di IA, poiché comporta rischi legati alla trasmissione di dati al di fuori del contesto delle cure, all'identificazione di persone nonché all'archiviazione e alla sicurezza dei dati. Al contempo, l'addestramento di questi modelli non risponde direttamente alle esigenze concrete e immediate della persona assistita. Anche nel caso in cui il riutilizzo dei dati è comunicato in modo trasparente, rimane problematico nell'ottica della proporzionalità dato che non è adeguato né necessario alla cura dei pazienti. Questo tipo di trattamento risulta quindi illecito, a meno che non sia possibile far valere un motivo giustificativo. Tuttavia, considerato il contesto e l'intensità del trattamento, sembrerebbe difficile giustificare il riutilizzo dei dati con un interesse preponderante. Resterebbe quindi solo il consenso della persona assistita, tenuto conto di tutte le limitazioni esposte precedentemente[6] (cfr. n. III 2).

8. Ulteriori elementi

Nel contesto della sorveglianza bisogna considerare anche altri elementi, alcuni dei quali esulano dall'ambito della protezione dei dati. I paragrafi seguenti delineano tali aspetti senza però trattarli in modo approfondito.

Per prima cosa, come già accennato, le misure di sorveglianza non interessano soltanto le persone assistite ma in particolare anche i visitatori e il personale della struttura, che devono essere adeguatamente informati in merito a questi sistemi e se del caso avere la possibilità

[6] Qualora gli algoritmi e l'IA siano stati addestrati con dati grezzi provenienti dall'estero, la responsabilità ricade sul produttore, tanto più che per i titolari del trattamento in Svizzera risulta difficile valutare la legittimità dei trattamenti ai sensi del diritto straniero.

di disattivarli. Per quanto riguarda il personale, si rimanda alle norme che disciplinano la sorveglianza nei rapporti di lavoro.

Un'ulteriore questione è quella della sorveglianza all'interno di spazi condivisi da più persone assistite (in particolare appartamenti, camere comuni e bagni). Senza entrare nei dettagli, queste situazioni risultano delicate. Come menzionato precedentemente, la sorveglianza deve essere adeguata al caso specifico. Di conseguenza, se essa non è giustificata in linea di principio o nella sua portata anche per le altre persone assistite, è opportuno rinunciarvi.

Inoltre, in determinati casi le misure di sorveglianza possono essere considerate come delle prescrizioni mediche. È quindi necessario tenere conto anche delle norme applicabili in questo ambito, in particolare per quanto riguarda il consenso (ipotetico, presunto, per rappresentanza). In altre circostanze la sorveglianza può anche assumere la natura di misure coercitive, limitando la libertà della persona assistita. Anche in questo caso possono applicarsi norme specifiche.

Qualora si ricorra a terzi per la sorveglianza, gli enti rimangono pienamente responsabili del trattamento dei dati. Si ha un caso di esternalizzazione del trattamento dei dati, ad esempio, quando viene utilizzato uno strumento di un fornitore di servizi per la sorveglianza o una soluzione cloud. In tal caso, occorre rispettare i requisiti giuridici specifici per il trattamento dei dati da parte di terzi. I terzi coinvolti possono trattare i dati solo nei limiti consentiti all'ente stesso. Oltre ai rischi derivanti dalle maggiori possibilità di accesso e dalla più ampia cerchia di persone coinvolte, possono sorgere ulteriori rischi qualora il trattamento dei dati avvenga all'estero. In questi casi, il responsabile del trattamento potrebbe essere soggetto a un ordinamento giuridico che non garantisce un livello adeguato di protezione dei dati. Ciò deve essere tenuto in considerazione nella definizione delle misure tecniche e organizzative.

9. Valutazione d'impatto sulla protezione dei dati e consultazione preventiva

Una valutazione d'impatto sulla protezione dei dati (VIPD) consente di individuare e valutare i rischi legati alla protezione dei dati. Inoltre, può aiutare a valutare la proporzionalità e a individuare misure volte a ridurre l'intensità del trattamento dei dati.

Sia la LPD che la maggior parte delle leggi cantonali sulla protezione dei dati prevedono che i titolari del trattamento debbano effettuare una VIPD, a determinate condizioni.

Gli enti privati soggetti alla LPD devono, ai sensi dell'art. 22 cpv. 1 LPD, redigere una VIPD se il trattamento può comportare un rischio elevato per la personalità o i diritti fondamentali della persona interessata. Tale rischio può essere indicato, in particolare, dal fatto che vengano trattati su larga scala dati personali particolarmente sensibili.

L'obbligo di redigere una VIPD per gli enti pubblici è disciplinato dalle disposizioni cantonali applicabili. Alcuni cantoni prevedono che debba essere redatta una VIPD per ogni nuovo trattamento di dati pianificato, mentre altri cantoni, analogamente alle disposizioni del diritto federale, richiedono la redazione di una VIPD solo se il trattamento di dati previsto comporta presumibilmente un rischio elevato per la personalità o i diritti fondamentali della persona interessata.

Una VIPD contiene in linea di principio una descrizione delle finalità del trattamento dei dati, una descrizione del trattamento previsto (elenco delle fasi di trattamento e dei luoghi in cui avviene il trattamento) e una valutazione dei rischi per la personalità o i diritti fondamentali della persona interessata (valutazione della probabilità di verificarsi e dell'entità del danno previsto). Per i rischi individuati dovrebbero inoltre essere definite delle misure, che vanno anch'esse elencate nella VIPD. Con l'ausilio di una tale VIPD è possibile tenere conto già nella fase di pianificazione e sviluppo delle ripercussioni del trattamento dei dati sugli interessati e valutare meglio la proporzionalità. La redazione di una VIPD può rivelarsi necessaria in particolare anche in caso di modifiche significative ai trattamenti esistenti, ad esempio a seguito della sostituzione di attività manuali o dell'introduzione di nuove tecnologie. In tal caso, la VIPD deve contenere un confronto quantitativo e qualitativo tra i trattamenti esistenti e quelli previsti.

L'articolo 23 capoverso 1 della LPD prevede che si debba richiedere un parere all'IFPDT, ai fini di una consultazione preventiva, qualora, nonostante le misure adottate, sussista ancora un rischio elevato per la personalità o i diritti fondamentali delle persone interessate. In caso di controversia, l'IFPDT può emettere un parere d'ufficio. Anche le leggi cantonali sulla protezione dei dati prevedono un controllo preventivo, sebbene i requisiti possano variare leggermente a seconda del diritto applicabile dalle autorità cantonali di protezione dei dati. Poiché il controllo preventivo deve essere effettuato prima dell'inizio del trattamento dei dati previsto, è opportuno prevedere un tempo adeguato.

IV. Obbligo di documentazione e guide TOM

In ogni caso, al momento dell'avvio del progetto i titolari del trattamento sono tenuti a effettuare un confronto tra le diverse soluzioni disponibili, includendo anche una valutazione dei rischi nell'ottica della protezione dei dati. Queste attività devono essere documentate per scritto e completate di pari passo all'avanzamento del progetto, nonché rivalutate regolarmente una volta che il sistema è stato implementato.

In particolare, è necessario attuare misure tecniche e organizzative adeguate (crittografia, controllo degli accessi, verbalizzazione). Si rinvia in tal senso alle guide ai provvedimenti tecnici e organizzativi concernenti la protezione dei dati (TOM) che saranno pubblicate da privatim e dall'IFPDT.

V. Lista di controllo

1. Identificare le necessità, in particolare nell'ottica del motivo giustificativo. Coinvolgere fin da subito gli specialisti interessati (giuristi, consulenti per la protezione dei dati, informatici, assistenti, ecc.).

2. Confrontare le diverse soluzioni disponibili, in particolare nell'ottica della tecnologia, e valutare i rischi (aspetti tecnici e giuridici).

3. Accertarsi di comprendere le capacità della soluzione scelta e, se del caso, delle opzioni di configurazione.

4. Sviluppare un piano d'attuazione coerente e un regolamento per l'uso (quando attivare la sorveglianza, chi può accedere ai dati, come informare le persone assistite, eventuale consenso, ecc.).

5. Formare il personale.

6. Occuparsi dell'attuazione concreta (cartelli informativi, ecc.).

7. Sviluppare un piano di controllo successivo e di rivalutazione del sistema.

Durante l'intero processo: redigere, completare e mantenere aggiornata la documentazione pertinente, in particolare le analisi dei rischi, i regolamenti ecc.

16.09.2026