La sanità deve fare a meno dei dati personali

✍🏻 Christian Bernieri
📝 29 maggio 2024

Indice dei contenuti:

Premessa

I baci non sono tutti uguali, così come gli amori non sono tutti uguali.

Ci sono situazioni che si ricordano per tutta la vita, che si distinguono dalle altre e che, lo sai già sin dall'inizio, non saranno mai più eguagliate da nulla di ciò che ti potrà capitare in futuro.
Sono sensazioni uniche e si vive per quei momenti, si spera che ogni giorno nasconda una di quelle perle, di quei personalissimi tesori per i quali si affronta con gioia e speranza ogni mattina, come se fosse un nuovo inizio.

Purtroppo, certe volte capita di pescare una carta "imprevisti" e le cose prendono una piega decisamente differente.

Le delusioni e i dolori non sono tutti uguali.
Alcuni passano in fretta.
Altri non si cancellano mai e sono senza rimedio.

I dati personali non sono tutti uguali e questo vale anche per i data breach.
Certi data breach sono senza rimedio, in particolare lo sono quelli che riguardano i dati relativi alla salute, alla vita sessuale o all'orientamento sessuale.

Questi dati particolari, questi dati sensibili, ci rendono particolarmente vulnerabili in modi che spesso non sappiamo prevedere e che dipendono da chi li avrà a disposizione e dall'uso malizioso/deteriore/deprecabile che saprà escogitare.

Siamo tutti bravi ragazzi e mediamente poco abili nell'uso degli strumenti informatici; per questo facciamo fatica a immaginare che ci siano persone malvagie e capaci di fare miracoli con un computer, ma la realtà è questa.

Un caso immaginario, ma non troppo

Prendiamo, per esempio, il caso di **Ingenuolo**, l'ottavo nano. Ingenuolo usa il computer solo al lavoro e pensa che il massimo che si possa fare sia saper usare bene un foglio Excel e nuotare nell'immenso mare del web. Ingenuolo non sa, però, che c'è tanta gente in gamba, capace di navigare con destrezza in rete con strumenti che lui nemmeno conosce, capace di estrarre dati da posti di cui ignora l'esistenza e di fare del male ben oltre le remore morali di Ingenuolo.

Quando i dati sensibili di Ingenuolo saranno nelle mani di un criminale informatico, inizierà quello che, in gergo, si chiama "*Pig Butchering*": la macellazione del porco. Rende l'idea? Ingenuolo sarà devastato in tutti i modi possibili, con totale noncuranza di ogni conseguenza. L'unico obiettivo sarà spolparlo fino all'ultimo brandello di valore.

Ingenuolo dovrà pagare per non far arrivare al suo datore di lavoro le sue cartelle cliniche, contenenti i dati relativi a quella brutta malattia che lo renderà sempre meno produttivo nei prossimi anni.
Una malattia invalidante, in molti Paesi, è discriminante per il datore di lavoro.

Ingenuolo dovrà pagare per non far sapere a sua moglie/figlia/madre/colleghi/tutto-il-mondo che soffre di questa o quella patologia o disfunzione imbarazzante. O che ne ha sofferto in passato.
Essere portatori di una patologia particolare può minare autostima e produttività, finanche diventare motivo di bullismo o mobbing.

Ingenuolo dovrà pagare per non far arrivare alle sue assicurazioni la documentazione che annullerà ogni copertura.
Stipulare una polizza assicurativa senza dichiarare di soffrire di una certa malattia, costituisce anche un reato e pregiudica qualsiasi tipo di copertura. Presente, futura e, spesso, anche passata.

Ingenuolo dovrà cambiare casa perché non gli è stato rinnovato l'affitto. Pare che il proprietario non gradisca affittare a persone con un particolare orientamento sessuale che, adesso, tutti conoscono.
Purtroppo la banca non approverà mai il mutuo che è stato chiesto perché Ingenuolo

non è un cliente come gli altri, è completamente trasparente a chi deve valutare il rischio connesso alla restituzione del denaro. La fede calcistica, il titolo di studi, il nome da nubile della madre non sono discriminanti ma lo stato di salute sì, eccome.

Ingenuolo si era anche candidato in un partito che professa posizioni radicali rispetto ad alcuni trattamenti sanitari. Ingenuolo dovrà rinunciare perché i criminali hanno venduto al partito avversario informazioni e documenti che testimoniano il suo ricorso a quelle stesse pratiche mediche che pubblicamente avversa.

Ingenuolo potrà essere ricattato in modi che solo una mente perversa può immaginare e che lo sorprenderanno. Non si capaciterà di quanto possa essere cattivo un essere umano.

Ingenuolo sarà disperato e probabilmente cliccherà su ogni email amica che gli proporrà un prestito in denaro oppure una consulenza per difendersi dai criminali informatici, installerà qualsiasi software di analisi per vedere se i suoi sistemi sono sicuri e pagherà cifre importanti per farsi aiutare. Ingenuolo non riuscirà a capire che dietro queste offerte ci sono proprio i suoi aguzzini.

Ah, naturalmente, mentre Ingenuolo si interfaccerà con i suoi macellai, si esporrà anche ad invisibili attacchi diretti e, senza accorgersene, il suo computer verrà compromesso, le sue password saranno note ai criminali, i suoi account saranno a lui preclusi e **nelle mani dei cattivi**, il contenuto del suo hard disk verrà copiato e poi bloccato.

A questo punto Ingenuolo potrebbe cominciare a capire come funzionano gli ingranaggi di questa arancia meccanica digitale e immaginare che domani, appena i criminali avranno setacciato bene i dati rubati, troveranno le foto porno che ha scaricato da internet, la sua cronologia su quei siti molto espliciti e molto particolari, le chat private in cui ha chiamato la moglie “troia”, la figlia “stronza” e il capo “coglione” … e intuirà che cosa lo aspetta. Ingenuolo vorrà smettere di esistere perché capirà che, purtroppo, non c’è altro modo per liberarsi di questo invincibile e spietato nemico invisibile.

Quella mattina Ingenuolo si era svegliato sperando di incontrare il più bel bacio ed il più bel giorno della sua vita ma, senza alcuna colpa, è precipitato all’inferno.

Tanti casi reali che superano l'immaginazione

Eccoci. Ingenuolo siamo noi, oggi.

Abbiamo tutti pescato una carta sfortunata e le conseguenze sono irrimediabili. Forse per questo stiamo tutti facendo finta che non sia successo nulla, che nulla stia capitando, ma ci siamo dentro fino alle orecchie.

"**Don't look up**": è profetico e parla di noi, clienti e utenti di aziende travolte dalla propria cialtronaggine. Noi, inermi vittime di data breach che hanno compromesso ciò che di più caro abbiamo: i nostri dati sensibili, affidati a soggetti incapaci di tutelarli come meritano e nel modo richiesto dalla legge.

I data breach sono tragedie collettive e devono essere valutati con i freddi parametri previsti dalla legge.

Questi stessi eventi, a livello individuale, vengono percepiti da ciascuno in modo molto diverso, a seconda delle ragioni che hanno portato i nostri dati a confluire nei database compromessi.

"**Mannaggia a me**": molti hanno deciso di fare prevenzione con un test diagnostico, di sottoporsi a cure volontarie o non strettamente necessarie. Hanno quindi deciso liberamente di registrarsi: fornire nome, cognome, dare l'assenso per essere inseriti in un database, nel gestionale di una clinica, tra i file di un dermatologo, ecc.

Chiunque si trovi in questa situazione dovrebbe biasimare se stesso, tuttavia siamo inclini a non farlo. Per questo valutiamo come la gravità di questi eventi in modo blando: "non è grave", "capita sempre", "tanto non ci fanno niente con quei dati". Minimizziamo anche perché, se la valutazione fosse più rigorosa e il giudizio più grave, faremmo molta fatica ad assolverci dalla nostra responsabilità. Se la colpa ci lambisce, se non possiamo più additare il fato, ci sentiamo molto stupidi. Non sia mai!

"**Pure questo mi tocca**": una fitta schiera di lavoratori, di assicurati che hanno denunciato un sinistro, di sportivi agonisti e di altre persone nella medesima situazione hanno dovuto fare visite e accertamenti, non per scelta, ma per obbligo di legge.

Molti lavoratori non hanno scelta e si devono sottoporre periodicamente a visite ed esami, spesso in centri medici o cliniche. Fa parte del lavoro ed è una misura di prevenzione obbligatoria.

Ogni rimborso assicurativo comporta la verifica di cartelle cliniche, referti medici, esami, a volte anche visite di controllo.

Sono in tanti, tra lavoratori, agonisti professionisti, a vivere sotto costante controllo medico.

Poi ci sono anche gli amatori, che si iscrivono in palestra o ad un'associazione sportiva dilettantistica e, anche solo per questo, devono fare visite, accertamenti ed esami. L'unica alternativa per evitarlo sarebbe dedicarsi ad altro, ma non sarebbe certamente la stessa cosa.
In questi casi la rabbia aumenta, non si ha alcun motivo per minimizzare e si cercano responsabilità tra quei soggetti che ci hanno obbligato ad avere a che fare con la sanità: il datore di lavoro, l'assicurazione, il centro sportivo. Rabbia che, tuttavia, sbiadisce rapidamente anche perché ci si rende conto che il problema si sarebbe manifestato identico anche con un altro datore di lavoro, un'altra assicurazione o un altro sport.

"**Che stronzi**": a volte non c'è scelta e ci si deve curare. Ciascuno, sotto sotto, si sente il primo di una nuova stirpe di immortali, ciascuno pensa di essere immune a tutto e di poter fare come il fantomatico nonno che è campato 103 anni fumando, bevendo e imprecando. Purtroppo non è così. I dati sanitari ci sono e crescono di anno in anno, ciascuno li alimenta con le piccole e grandi cose della vita e ogni informazione viene registrata. Chi ha dovuto affrontare la malattia è provato, esasperato, forse esausto ma non può tollerare di sentirsi una cavia, un semplice numero senza valore, una vittima designata dell'inettitudine o della cialtroneria. La rabbia scorre potente quando la colpa sta tutta sulle spalle di chi avrebbe dovuto prendersi cura di noi, aiutarci, assisterci.

"**Questi sono scemi nella testa**": a volte le cose si complicano. A volte, per due spicci, per poter usufruire di una micro deduzione dello zero virgola per cento, su un massimale di un pugno di €, da recuperare in millemila mini rate di rimborso, oppure per maturare ambitissimi "*punti fregala**", in pratica, per un'inezia decidiamo di strisciare il codice fiscale ad ogni acquisto, di registrarci ad ogni promozione e, così facendo, di lasciar proliferare i nostri dati in modo esponenziale. Forse, anche la nostra testa, giusta giusta non è.

**ironic mode on*

Tsunami
A prescindere dalla percezione individuale, mettendo per un attimo da parte considerazioni del tenore di "*io non l'ho mai visto*" e "*a me non è mai capitato*", l'entità del fenomeno deve fare spavento.

Alla mia famigerata memoria viene in soccorso Ransomfeed che tutto registra e documenta. Questi sono i data breach occorsi negli ultimi mesi.

Synlab, 04.05.2024
https://ransomfeed.it/index.php?page=post_details&id_post=15161
Uno dei peggiori della storia, ancora in corso nel momento della scrittura di questo pezzo. I criminali informatici (Blackbasta) hanno copiato 1,5 TERABYTE di dati per la consueta estorsione (paga o li pubblichiamo) e hanno messo KO tutti i sistemi informatici dell'azienda. Per alcune settimane, non ha funzionato nulla, computer, server, sito web, centralino, sistemi di posta... niente. Non hanno risparmiato niente. Non possiamo prevedere come si svilupperà questo data breach ma una cosa è certa: in quei 1.500 Gigabyte di dati, ci sono i dati sensibili di centinaia di migliaia di persone, forse milioni.

Croce Rossa, presunto aprile 2024
https://breachforums.st/Thread-Italian-Red-Cross-Breach
Un data breach interno ad una sezione della Croce Rossa che ha esposto tutti i dati contenuti in un computer accessibile dall'esterno. Password banali, utilizzate identiche su vari sistemi, protezioni assenti. Non si può nemmeno parlare di violazione dei sistemi: sono praticamente aperti su internet, basta entrare.

Farmacia Ettore Florio, 08.04.2024
https://ransomfeed.it/index.php?page=post_details&id_post=14162
A livello locale, una farmacia colleziona i dati di un'intera città. Tutti ci passano, acquistano, prenotano farmaci, accedono a servizi, attivano tessere a punti, prenotano esami. Su scala locale, una tragedia e, in questo caso, una tragedia ancora più estesa dato che la farmacia colpita ha una intensa attività di vendita online: 300 Gigabyte di dati personali sensibili.

Associazione Veterinari ed Igienisti Italiani, 19.02.2024
https://ransomfeed.it/index.php?page=post_details&id_post=13363
Un database di cui non si sa molto ma collegato al mondo della sanità. Un'associazione di categoria del settore.

Azienda Sanitaria Locale Basilicata, 15.02.2024
https://ransomfeed.it/index.php?page=post_details&id_post=13301
Una bomba atomica sulla sanità della Basilicata ed una delle pagine più tristi della comunicazione di crisi. In pochi istanti, la sanità regionale è tornata all'età della pietra,

senza alcuna infrastruttura funzionante. Niente più email, niente agenda, niente prenotazioni, niente cartelle cliniche, niente di niente. I dati (circa mezzo terabyte) sono stati compromessi, copiati ed è scattata l'estorsione per non pubblicarli.

Azienda Sanitaria Locale Modena, 11.12.2023
https://ransomfeed.it/index.php?page=post_details&id_post=12315
Altra incredibile pagina di mistificazione collettiva: enti ed istituzioni che hanno fatto di tutto per minimizzare, per rassicurare e per negare l'esistenza di un rischio. In questa situazione, le persone coinvolte, le vere vittime, non meritavano di essere prese in giro da dichiarazioni e comunicati stampa raccapriccianti.
Anche in questo caso, sistemi bloccati per settimane, dati rubati e pubblicati.

Centro Ortopedico Il Quadrante, Ospedale COQ, 05.11.2023
https://ransomfeed.it/index.php?page=post_details&id_post=11682
Piccolo centro ospedaliero che, a livello locale, raggruppa i dati relativi alla salute di ogni persona della valle.

ASL Verona, Ottobre 2023
https://www.larena.it/news/veneto/attacco-hacker-ospedale-verona-1.10348922
Blocco di ogni sistema, accessibilità dei servizi online e all'interno delle strutture, settimane di lavoro per recuperare operatività.

Ordine degli Psicologi della Lombardia, 10.10.2023
https://ransomfeed.it/index.php?page=post_details&id_post=11269
Da uscire di testa: 5 gigabyte di dati rubati e relativi ai professionisti iscritti all'Ordine.

Istituto Prosperius, 26.09.2023
https://ransomfeed.it/index.php?page=post_details&id_post=11084
Rubati e venduti online i dati del noto centro medico, di lavoratori e pazienti.

Clear MediCare, 26.06.2023
https://ransomfeed.it/index.php?page=post_details&id_post=8552
Data breach nel settore privato che, sebbene meno colpito, non è decisamente immune.

Azienda Sanitaria Locale Avezzano, Sulmona L'Aquila 1, 03.05.2023
https://ransomfeed.it/index.php?page=post_details&id_post=7658
Uno dei data breach più eclatanti e più discussi: 500 Gigabyte di dati di utenti e

pazienti, praticamente tutta la sanità regionale compromessa. Tutti i dati sono stati pubblicati nonostante l'intervento di ogni possibile autorità pubblica. Anche in questo caso la ASL ha minimizzato, anzi, nascosto gli eventi, al punto da richiedere un intervento diretto del Garante per obbligare i dirigenti a informare le persone coinvolte del fatto.

Gruppo MultiMedica, 27.04.2023
https://ransomfeed.it/index.php?page=post_details&id_post=7559
Grande azienda che gestisce ambulatori e centri ospedalieri, centinaia di migliaia di utenti coinvolti e dati pubblicati online. Una tragedia.

Hospital Service, 14.02.2023
https://ransomfeed.it/index.php?page=post_details&id_post=6049
50 gigabyte di dati rubati ad un grande centro della sanità romana.

Azienda Ospedaliera di Alessandria, 28.12.2022
https://ransomfeed.it/index.php?page=post_details&id_post=5625
1 TERABYTE (1000 Gigabyte) di dati rubati all'Azienda Ospedaliera.

Ospedale Macedonio Melloni, 21.06.2022
https://ransomfeed.it/index.php?page=post_details&id_post=4058
Grande ospedale nel cuore di Milano, dati

Azienda Sanitaria di Messina, 21.04.2022
https://ransomfeed.it/index.php?page=post_details&id_post=3441

ASL Cosenza, Febbraio 2022
https://www.asp.cosenza.it/?p=articoli&id=1943-a-tutti-i-dipendenti-asp-cosenza-alcuni-servizi-interni-dell-asp-di-cosenza-sono-interrotti-per-pr
Disservizi, blocchi e dati rubati. Periodaccio per le ASL.

Farmacia Statuto, 10.04.2022
https://ransomfeed.it/index.php?page=post_details&id_post=3293

Unità Locale Socio Sanitaria di Padova, 24.01.2022
https://ransomfeed.it/index.php?page=post_details&id_post=2490

Azienda Sanitaria Locale Napoli 3, 14.01.2022
https://ransomfeed.it/index.php?page=post_details&id_post=2490

Azienda Sanitaria Locale Veneto 6, 01.01.2022
https://ransomfeed.it/index.php?page=post_details&id_post=2490

E via perdendosi nella notte dei tempi.

La dura verità

La verità, purtroppo, è che dietro ad ogni data breach c'è solo la spietata legge dei grandi numeri.
Siamo tanti, tantissimi, siamo troppi da gestire con le scarse risorse che abbiamo a disposizione. I grandi numeri richiedono logiche di analisi, efficientamento e razionalizzazione che di umano conservano ben poco e che richiedono molti dati, anzi, TUTTI i dati.

La gestione della spesa sanitaria è governata dall'analisi dei dati. I protocolli di cura sono fortemente condizionati dai dati. L'organizzazione stessa delle risorse è basata sui dati. Gli unici investimenti che vengono realizzati riguardano proprio gli strumenti di acquisizione, condivisione e analisi dei dati sanitari, prima ancora che le risorse necessarie per l'erogazione delle cure. Questo perché la legge dei grandi numeri implica la necessità di ottenere il massimo risultato con il minimo sforzo.

Oggi, in tutto questo, la protezione dei dati non è affatto contemplata.
Ma tutto ciò è anche una precisa scelta politica e, quindi, può cambiare.

La complessità dei sistemi, la quantità di dati sia a livello periferico che centralizzato, la loro condivisione tra soggetti variamente affidabili, la cialtronaggine che, per natura, si incontra lungo la propria strada, la scarsità di risorse investite nella protezione e il costante, sempiterno primato dell'approccio reattivo, a danno dell'approccio preventivo, completano il quadro della catastrofe introducendo ogni possibile vulnerabilità nota all'uomo.. e infinite altre, non ancora rivelate.

Criminali dal cuore d'oro

Come se questo non bastasse, nemmeno le vulnerabilità sono tutte uguali. Alcune sono peggiori di altre, alcune meno note di altre, alcune più recenti di altre e ve ne sono alcune, talmente costose da gestire, che ci si rifiuta persino di volerle prendere in

considerazione. Purtroppo, la solidità di un sistema è pari al suo anello più debole e, quindi, sarà sempre la peggiore tra le vulnerabilità, la più trascurata a mettere in crisi tutti i dati personali contenuti nei sistemi della sanità pubblica e privata. Di solito, questa vulnerabilità coincide con il "**fattore umano**".

Per parafrasare il manifesto della **convention hacker del 2009 di Wellington**, possiamo dire serenamente che i criminali dal cuore d'oro appartengono ad un immaginario confortante ma irreale.
Ad un criminale informatico non importa proprio nulla di tante cose…

- *Dello scopo meritorio e importantissimo del tuo sistema informatico*
- *Se è gestito da un fornitore terzo, magari inadeguato*
- *Se è un sistema obsoleto o ereditato dalla precedente gestione*
- *Se è un sistema troppo critico per intervenire con migliorie che potrebbero creare dei blocchi*
- *Del DOWN time, ovvero di quanto dovrai tenere fermo un sistema per ripristinarlo*
- *Del tuo budget*
- *Se hai sempre fatto in un certo modo*
- *Della data prevista dai tuoi piani di sviluppo*
- *Se un sottosistema vulnerabile è solo un esperimento o una prova per vedere come funziona*
- *Degli accordi di non divulgazione e riservatezza e di tutta la carta firmata tra i partner*
- *Se nel contratto non sono indicati alcuni requisiti essenziali di protezione*
- *E nemmeno se nel contratto era stato previsto ogni requisito, magari non ancora attuato*
- *Se è un sistema solo interno, non destinato a finire online*
- *Se è davvero difficile cambiare qualcosa perchè lo sviluppatore non c'è più*
- *Se è dovuto a sostituzioni e cambiamenti in corsa e in emergenza*
- *Se non sei sicuro di come fare a migliorare o proteggere i dati*
- *Se è gestito nel Cloud*
- *Di come hai stimato il rischio*
- *Se il tuo fornitore non supporta una determinata configurazione e, per questo, hai aperto porte che dovevano restare chiuse*
- *Se attualmente gira una soluzione temporanea, in attesa di quella fighissima e definitiva*
- *Se hai una certificazione ISO UNI EN… [inserire qui standard a piacimento]*
- *Se i dati sono crittografati solo durante il trasferimento*

- *Se il bilanciamento costi benefici è sfavorevole*
- *Se diremo «Nessuno mai poteva immaginarselo»*
- *Se non puoi sacrificare «il Business» per un rischio potenziale e solo teorico*
- *Se hai altre priorità oppure se il problema compete a qualcun altro*
- *Dell'affidabilità e della competenza del tuo staff*
- *Se non hai alcuna motivazione commerciale o di mercato per migliorare*
- *Se non puoi calcolare un Return on Investment*
- *Se hai esternalizzato un determinato rischio*

Un criminale informatico è e sarà sempre in vantaggio su di noi, illusi che esista compassione.

La grande abbuffata
Per non soccombere è necessario un cambio radicale di prospettiva: è necessario che ogni server ed ogni computer aggredito sia vuoto o che esponga al rischio solo un contenuto minimale.
I dati, semplicemente, **non ci devono essere**.

Oggi facciamo il contrario e abbiamo una bulimia di dati, così abbondanti che il solo quantificarli richiederebbe calcoli quantici.

Un esempio per tutti.
Poco tempo fa, mia moglie è stata ricoverata in ospedale per il parto di nostra figlia.
All'accettazione la zelante signorina ci ha accolto con le domande di rito.
"*Buongiorno e benvenuta.*"
"*Mi dia pure la sua tessera sanitaria.*"
"*Intanto che la registro, le do alcuni moduli da leggere..*"
"*Ah, vedo che è già stata ricoverata qui da noi.*"

SDENG!

"*No, guardi, si sbaglia, sarà un'omonima, io non sono mai stata ricoverata, glielo garantisco.*"
"*Ma sì, signora, qui c'è la sua scheda, vede? Dimessa il 1 gennaio 1975, peso 2,050 chilogrammi...*"
"*Signora, guardi che è quando sono nata.*"

:-0

Ecco, non sarà **un po' troppo**?
È veramente necessario che dati come questi siano nel server, immediatamente disponibili, accessibili e in linea dopo 40 anni? Che fine ha fatto il principio della minimizzazione dei dati previsto dall'art 5 del GDPR?
Attenzione: nessuno pensa che i dati debbano scomparire, ma che senso ha renderli tutti permanentemente online?
È questo che dovrà cambiare se vogliamo davvero proteggerci dal disastro.

Dobbiamo smettere di pensare che le macchine ci possano tutelare meglio di quanto possiamo fare noi. I nostri dati devono essere in casa nostra, in una cartellina. Possono essere anche in ospedale, ma sempre in una cartellina o in un sistema di archiviazione segregato e distinto da quelli in produzione. Minimizzare i rischi significa fare in modo che, se c'è un furto di dati, ne vengano rubati il meno possibile. Esporre al rischio TUTTI i dati è una follia perché qualsiasi danno scala ad un livello collettivo.

Pensare che un software, un gestionale o un server possa proteggere i nostri dati in modo adeguato significa non rendersi conto che quel programma e quella macchina rispondono a logiche differenti, che sono stati predisposti da persone con obiettivi differenti e che la protezione è solo uno dei tanti task che il programmatore doveva realizzare, non certo quello prioritario e, anzi, probabilmente antitetico rispetto ad altri task come la velocità del sistema, la fluidità dei processi, l'assenza di blocchi, la minimizzazione delle chiamate di assistenza, ecc.

Meno dati = meno rischi

La prossima volta che andremo in un grande centro diagnostico, in uno studio odontoiatrico, in una clinica, dovremo provare a fare caso a quanti dati sono già in loro possesso, online, nel computer accessibile dalla prima persona che ci accoglie e da tutte le altre persone che seguiranno il nostro trattamento.
Perché chi ci stampa i referti deve poter vedere anche i referti precedenti?
Perché nella nostra area utente del fighissimo portale online, per scaricare i referti in autonomia, possiamo vedere più informazioni su di noi di quelle che conosce nostra madre?
Perché all'accettazione vedono la cartella clinica di quando è nata mia moglie?

Già... la prossima volta.
Di nuovo speriamo in un roseo domani, in una nuova alba di gioia e speranza.

Iniziamo oggi. Iniziamo negando il consenso. Sempre e comunque.

E all'obiezione "*Signora, è per la sua comodità, così trova tutto nella sua area utente*" potremo tranquillamente rispondere "***APPUNTO***!"

Un tempo, le automobili venivano pubblicizzate facendo leva sulla velocità massima raggiunta, l'accelerazione, i cavalli.
Oggi le pubblicità riguardano la sicurezza, l'affidabilità, l'autonomia o i costi di esercizio, l'impatto ambientale.

Quando le persone cominceranno a manifestare consapevolezza su questi temi, a comportarsi in modo più attento, quando le autorità di controllo faranno il loro lavoro (creando cultura della protezione dei dati personali, sanzionando chi non rispetta i principi del GDPR e orientando l'attività legislativa), quando "la privacy" diventerà una figata, un valore da tutelare, allora le aziende inizieranno a vendere privacy e garantiranno maggiori standard di protezione dei dati personali.