PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4880 di Venerdì 26 febbraio 2021

La pseudonimizzazione: una tecnica di protezione dei dati ancora poco nota

L'Agenzia europea per la sicurezza dei sistemi informativi-ENISA, ha recentemente pubblicato un prezioso documento, che illustra una tecnica di protezione dei dati ancora poco nota e poco utilizzata dagli esperti.

L'articolo 4 del regolamento europeo, che illustra le definizioni dei vari termini utilizzati in prosieguo, offre una chiara definizione di questo termine:

5) "pseudonimizzazione": il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

È bene chiarire subito che tra questa definizione e quella di dato anonimo vi è una significativa differenza, come è stato chiaramente evidenziato fin dal 2014 nell'opinione 5 dell'articolo 29 Working party.

Un dato pseudonomizzato non può essere considerato equivalente ad una informazione resa anonima, perché nel primo caso è ancora possibile ricostruire il dato del singolo interessato, mentre nel secondo caso l'operazione dovrebbe risultare irreversibile.

L'argomento è preso in considerazione in numerosi punti del regolamento generale europeo, ed in particolare nei seguenti Considerando: 26 28 29 75 85 156.

Dovrebbe bastare questo fatto per sottolineare quanto sia importante questo tema e deplorare il fatto che, almeno fino ad oggi, esso venga utilizzato raramente.

Il tema viene nuovamente ripreso nell'articolo 32, dedicato alla sicurezza del trattamento, laddove al comma 1, lettera a) si fa specifico riferimento a questa tecnica di protezione dati personali, abbinata alla cifratura.

Non deve pertanto stupire il fatto che ENISA abbia recentemente pubblicato un prezioso documento, che illustra ai titolari e responsabile del trattamento, nonché al responsabile della protezione dei dati, quali sono le tecniche utilizzabili, illustrandone

pregi e difetti.

Il documento riprende degli studi che la stessa agenzia europea aveva sviluppato in passato, e rappresenta un riferimento praticamente obbligatorio per tutti coloro che vogliono utilizzare questa preziosa tecnica di protezione dei dati personali.

Tanto per cominciare, l'agenzia mette in guardia sul fatto che questa tecnica è solo una di quelle che possono essere utilizzate e deve essere sempre accompagnata da una valutazione del rischio, afferente alla situazione specifica.

D'altro canto, la relativa semplicità di applicazione di tecniche di protezione di questo tipo rende particolarmente attraente questa tecnologia nel settore della sanità, che ormai è tristemente famosa in tutto il mondo per le vistose carenze, in termini di protezione dei dati, che più volte purtroppo si sono manifestate.

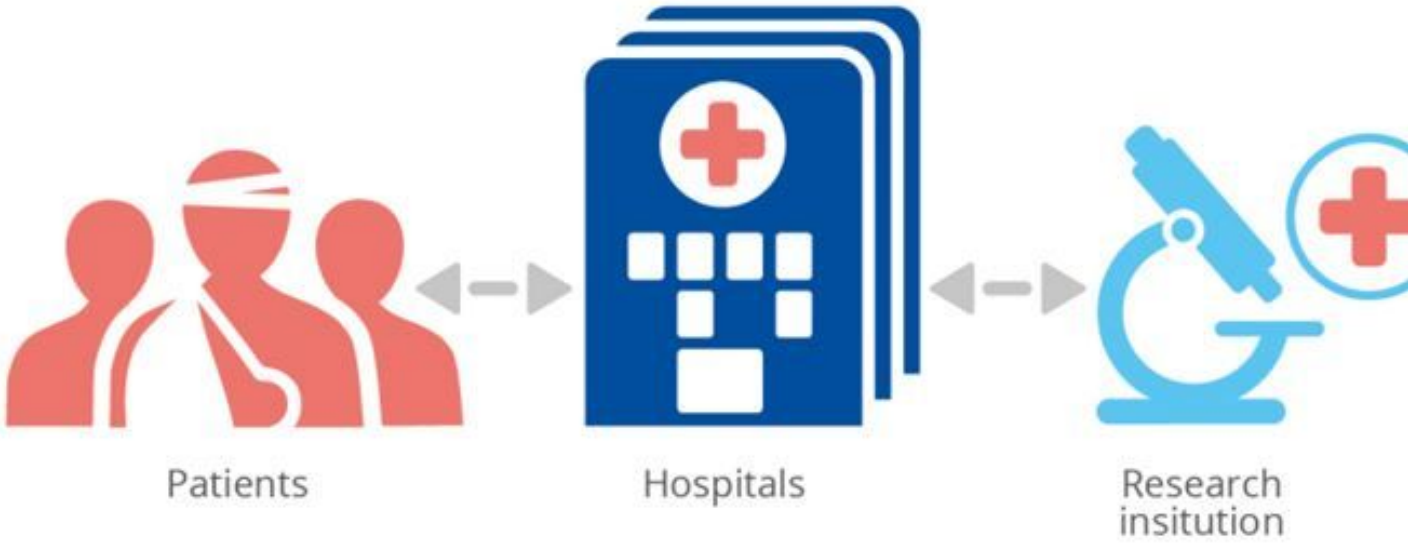
Lo studio mette in evidenza che non esiste una tecnica unica da utilizzare, ma occorre sempre effettuare un'analisi specifica del contesto specifico, per scegliere l'opzione più appropriata, tra le numerose disponibili.

Il documento dapprima offre una panoramica delle tecniche più correntemente utilizzate, passando quindi, nel terzo capitolo, ad illustrare un certo numero di tecniche avanzate, compresa la crittografia asimmetrica ed altre tecniche specifiche. Trattandosi perlopiù di tecniche di origine anglosassone, riporto di seguito senza traduzione i termini originali:

"ring signatures, chaining mode, Merkle trees, pseudonyms with proof or ownership, secure multiparty computation and secret sharing schemes."

Il quarto capitolo è interamente dedicato a queste tecniche applicate al mondo della sanità, per le ragioni che sono stati illustrate in precedenza.

Come noto, il mondo della sanità deve spesso ricorrere all'utilizzo dei dati personali dei pazienti, al fine di sostenere studi specifici, miranti ad inquadrare e mettere sotto controllo malattie di vario tipo. In questo caso, gli istituti di ricerca hanno bisogno di avere a disposizione un gran numero di dati personali di pazienti, ma non necessariamente di conoscere nome e cognome dei pazienti coinvolti. Ecco perché, se da un lato è del tutto comprensibile che gli ospedali possano cedere dati personali di pazienti, ai fini del potenziamento della ricerca medica, dall'altro lato è altrettanto importante che l'identità dei pazienti venga



tutelata.

Il capitolo 5 illustra l'applicazione di queste tecniche nel più generale mondo delle tecnologie di sicurezza informatica, mentre l'ultimo capitolo riepiloga tutti i temi precedentemente trattati e offre specifiche raccomandazioni a tutti coloro che desiderano arricchire le proprie conoscenze su questo tema, al fine di utilizzare al meglio queste tecniche, nella protezione dei dati personali.

Particolarmente interessante è il fatto che più volte questo documento fa appello alla commissione europea e ad altre agenzie europee per offrire a titolari e responsabili del trattamento delle indicazioni e delle illustrazioni specifiche, in modo da favorire un utilizzo allargato di queste tecniche.

Purtroppo, ancora una volta, il documento è disponibile solo in lingua inglese, che ormai sta diventando la lingua standard per la diffusione di qualsiasi informazione afferente al trattamento protezione dati personali.

ENISA Report - Data Pseudonymisation - Advanced Techniques and Use Cases (pdf)

Adalberto Biasiotti
