SEPARAZIONE E CRIPTAZIONE DEI DATI IN AMBITO SANITARIO

SOMMARIO

Gli enti pubblici sono soggetti alla disposizione prescritta dall'**art. 22 comma 6**[1] del D. Lgs. 196/2003, in base alla quale i dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

Tale previsione prevede tre soluzioni alternative, il cui fine ultimo è l'inintelligibilità temporanea dei dati:

1. Cifratura dei dati oppure
2. Utilizzo di codici identificativi oppure
3. Utilizzo di altre soluzioni.

La scelta di una tra le soluzioni proposte deve in ogni modo condurre all'identificazione dell'interessato solo in caso di necessità.

La norma prevista dall'**art. 34 comma 1 lett. h)**[2] in materia di misure minime di sicurezza ribadisce il concetto espresso nell'art. 22 comma 6: prevede infatti

---

[1] Art. 22 (Principi applicabili al trattamento di dati sensibili e giudiziari)
(omissis)
6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

[2] Art. 34 (Trattamenti con strumenti elettronici)
1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
(omissis)

l'adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

L'**art. 22 comma 7**[3] prevede inoltre che i dati idonei a rivelare lo stato di salute e la vita sessuale siano conservati separatamente da altri dati personali che non richiedano il loro utilizzo, a prescindere dal fatto che siano organizzati in banche di dati.

La lettura delle norme citate permette di giungere alla conclusione che è obbligatoria la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dai dati personali dell'interessato, mentre non è obbligatoria la cifratura di tali dati sensibili, essendoci due soluzioni alternative: l'utilizzo di codici identificativi oppure l'utilizzo di altre soluzioni che rendano i dati intelligibili e che permettano l'identificazione dell'interessato solo in caso di necessità.

Le norme di carattere regolamentare integrano e specificano quanto appena detto. Ci si riferisce in particolare a quanto previsto dal **punto 24 dell'allegato B**[4].

Questa norma impone che le misure previste dall'art. 22 comma 6 debbano *anche* consentire il trattamento disgiunto dei dati idonei a rivelare lo stato di salute o la vita sessuale dagli altri dati personali che permettono di identificare direttamente gli interessati. E' un richiamo esplicito alla separazione dei dati prevista dall'art. 22 comma 7: la cifratura dei dati oppure l'utilizzo di codici identificativi oppure l'utilizzo di altre soluzioni deve accompagnare la separazione dei dati sensibili da quelli

---

h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

[3] Art. 22 ((Principi applicabili al trattamento di dati sensibili e giudiziari)
(omissis)
7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

[4] Allegato B al D. Lgs. 196/1003
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

personali e tali misure di sicurezza non possono rendere impossibile il trattamento disgiunto dei dati stessi.

La separazione dei dati e la cifratura degli stessi non sembrano quindi opzioni alternative, bensì cumulative, restando al titolare del trattamento la possibilità di optare per altre misure minime rispetto alla cifratura.

Le scelte possibili sembrano quindi essere le seguenti:

- Separazione + cifratura
- Separazione + codici identificativi
- Separazione + altre misure.

Tale interpretazione letterale, aderente al disposto della legge, è rafforzata, da un punto di vista sistematico, dalla lettura dell'art. 3 commi 4 e 5 del D. Lgs. 135/1999, che aveva provveduto ad integrare la L. 675/1996 in materia di trattamento di dati sensibili da parte di soggetti pubblici.

Nell'art. 3 comma 4 di tale decreto era infatti prescritto che i dati contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di mezzi elettronici, fossero trattati con tecniche di cifratura o mediante l'utilizzo di codici identificativi o di altri sistemi che permettessero di identificare i dati solo in caso di necessità. Il successivo comma 5 precisava che i dati idonei a rivelare lo stato di salute o la vita sessuale dovessero essere conservati separatamente da ogni altro dato personale trattato per altre finalità che non richiedessero il loro utilizzo.

Il **punto 19.8 dell'allegato B**[5] sembra però contrastare con tale ricostruzione. Infatti, per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, si richiede che nel DPS siano individuati *i criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.* Sembra sussistere un'alternatività che in realtà non esiste. L'opinione di chi scrive è che si tratti di un'imprecisione letterale del legislatore: sarebbe, infatti, stato lecito attendersi una "e" al posto di una "o", sia per confermare i dettami delle altre norme citate (in aderenza ad un'interpretazione strettamente letterale), sia per la

[5] Allegato B al D. Lgs. 196/2003
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

visione sistematica derivante dall'intero contesto in cui il nuovo corpus legislativo si è inserito.

Va criptata la trasmissione dei dati tra client e server?

Ai sensi dell'**art. 31 del D.Lgs. 196/2003**[6] sussiste un obbligo di sicurezza in capo al titolare del trattamento dei dati: i dati personali devono essere custoditi e controllati in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi che incombono sui dati stessi (distruzione, perdita, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta).

L'**art. 33 del codice**[7], nel quadro dei più generali obblighi di sicurezza previsti dall'art. 31, introduce il concetto di misure minime, vale a dire quelle misure che sono volte ad assicurare un livello minimo di protezione dei dati personali.

Il concetto di misura idonea differisce da quello di misura minima: l'inosservanza delle misure idonee può configurare una responsabilità civile (**art. 15 D. Lgs. 196/2003**[8]), mentre l'inosservanza delle misure minime è prevista come illecito penale ed è indipendente dal danno procurato.

La criptazione dei dati trasmessi tra client e server sembra essere tesa all'implementazione di una misura idonea di sicurezza, non di una misura minima.

Il punto di partenza è ancora l'art. 34 lett. h), il quale prevede come misura minima "l'adozione di tecniche di cifratura o di codici identificativi per determinati

---

[6] Art. 31 (Obblighi di sicurezza)
1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

[7] Art. 33 (Misure minime)
1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

[8] Art. 15 (Danni cagionati per effetto del trattamento)
1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari".

La misura minima di riferimento contenuta nell'allegato B è ancora il **punto 24**, il quale, dopo aver ribadito i principi dell'art. 22 comma 6 e 7, prosegue delineando una sicurezza più forte per i dati relativi all'identità genetica: essi possono essere trattati esclusivamente all'interno di locali protetti e accessibili solo da persone autorizzate; il trasporto dei dati all'esterno di questi locali può avvenire solo in contenitori muniti di serrature o dispositivi equipollenti; il trasferimento di tali dati in formato elettronico deve essere cifrato.

L'uso del *punto e virgola* da parte del legislatore lascia intendere che queste disposizioni si riferiscono soltanto ai dati relativi all'identità genetica e non a tutti i dati idonei a rivelare lo stato di salute e la vita sessuale oggetto del punto 24.

Il legislatore è stato molto chiaro nel delineare il quadro delle misure minime di sicurezza: se avesse voluto che tutti i trasferimenti di dati riguardanti la salute e la vita sessuale fossero criptati, l'avrebbe detto (ubi lex voluit, ubi tacuit noluit) e non avrebbe richiamato l'art. 22 comma 6 nello stesso punto 24, che prevede l'alternativa tra la criptazione, l'uso di codici identificativi e l'uso di altre misure.

E se anche fosse possibile estendere la portata della seconda parte del punto 24 a tutti i dati relativi alla salute e alla vita sessuale, non potendoci appellare per la comprensione ad una definizione di "trasferimento di dati", che nel codice non esiste, sarebbe necessario comprendere la disposizione analizzando il contesto in cui si trova.

I primi due enunciati riguardanti i dati relativi all'identità genetica si occupano della sicurezza fisica dei dati. In particolare, il secondo si occupa del trasferimento fisico dei dati all'esterno dei locali; sembra lecito pensare che anche il trasferimento elettronico dei dati debba essere inteso come trasferimento dei dati all'esterno della rete informatica e non ad un trasferimento dei dati tra client e server all'interno della rete stessa. Infatti, l'inaccessibilità dall'esterno della rete è comunque garantita contro l'accesso abusivo di cui all'art. 615 ter c.p. mediante idonei strumenti elettronici: questa è una misura minima obbligatoria.

La conclusione cui si giunge è che la criptazione della trasmissione dei dati tra client e server non costituisca una misura di sicurezza obbligatoria.

SEPARAZIONE E CRIPTAZIONE DEI DATI IN AMBITO SANITARIO

Si vuole però porre l'accento sull'opportunità di tale criptazione, alla luce delle conseguenze che potrebbero derivare in caso di danno cagionato per effetto del trattamento: la previsione della criptazione del trasferimento dati tra client e server come misura idonea e preventiva sarebbe una garanzia per l'ente pubblico in caso di giudizio in materia di responsabilità civile ex art. 2050 c.c..
Dal punto di vista di chi scrive sarebbe opportuno prevedere uno sviluppo dei software di refertazione ospedaliera in questa direzione.

Daniela Rocca
Studio Genghini & Associati